

National Aeronautics and Space Administration



---

# **Space Shuttle Independent Assessment Team**

---

Report to Associate Administrator  
Office of Space Flight

---

October - December 1999

March 7, 2000

**SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT**

---

This page intentionally left blank

# Table of Contents

<i>Table of Contents</i>	<i>ii</i>
<i>Independent Assessment Team Members</i>	<i>v</i>
<i>Acknowledgements</i>	<i>vi</i>
<b>Support Staff</b>	<b>vii</b>
<b>Technical Contributors</b>	<b>vii</b>
<b>Section 1 - Executive Summary</b>	<b>1</b>
<b>Issue 1</b>	<b>1</b>
NASA must support the Space Shuttle Program with the resources and staffing necessary to prevent the erosion of flight-safety critical processes.	1
<b>Issue 2</b>	<b>2</b>
The past success of the Shuttle program does not preclude the existence of problems in processes and procedures that could be significantly improved.	2
<b>Issue 3</b>	<b>2</b>
The SSP's risk management strategy and methods must be commensurate with the 'one strike and you are out' environment of Shuttle operations.	2
<b>Issue 4</b>	<b>3</b>
SSP maintenance and operations must recognize that the Shuttle is not an 'operational' vehicle in the usual meaning of the term.	3
<b>Issue 5</b>	<b>3</b>
The SSP should adhere to a 'fly what you test / test what you fly' methodology.	3
<b>Issue 6</b>	<b>4</b>
The SSP should systematically evaluate and eliminate all potential human single point failures.	4
<b>Issue 7</b>	<b>4</b>
The SSP should work to minimize the turbulence in the work environment and its effects on the workforce.	4
<b>Issue 8</b>	<b>5</b>
The size and complexity of the Shuttle system and of the NASA/contractor relationships place extreme importance on understanding, communication, and information handling.	5
<b>Issue 9</b>	<b>5</b>
Due to the limitations in time and resources, the SIAT could not investigate some Shuttle systems and/or processes in depth.	5
<b>Return To Flight</b>	<b>6</b>
<b>Section 2 - Charter</b>	<b>7</b>
<b>Guidance from Associate Administrator</b>	<b>7</b>

# SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT

<b>Section 3 - Introduction</b>	<b>8</b>
<b>Section 4 - Technical Sections</b>	<b>10</b>
<b>Technical Section Listing</b>	<b>10</b>
<b>Avionics</b>	<b>11</b>
<b>Human Factors</b>	<b>15</b>
<b>Hydraulics</b>	<b>20</b>
<b>Hypergols and Auxiliary Power Unit</b>	<b>23</b>
<b>Problem Reporting &amp; Tracking Process</b>	<b>27</b>
<b>Propulsion</b>	<b>37</b>
SSME, External Tank, Solid Rocket Booster, Reaction Control System	37
<b>Risk Assessment &amp; Management</b>	<b>46</b>
<b>Safety and Mission Assurance</b>	<b>51</b>
<b>Software</b>	<b>55</b>
Development & Maintenance	55
<b>Structures</b>	<b>57</b>
Airframe, Thermal Protection Systems, and External Tank	57
<b>Wiring</b>	<b>64</b>
<b>Section 5 - Recommendations</b>	<b>75</b>
<b>Category 1: Immediate</b>	<b>75</b>
Prior to Return to Flight	75
<b>Category 2: Short term</b>	<b>75</b>
Prior to making more than four more flights	75
<b>Category 3I: Intermediate term</b>	<b>77</b>
Prior to January 1, 2001	77
<b>Category 3L: Long term</b>	<b>79</b>
Prior to January 1, 2005	79
<b>Section 6 - Appendices</b>	<b>81</b>
<b>Appendix 1</b>	<b>82</b>
Rationale for Time Frames	82
<b>Appendix 2</b>	<b>83</b>
Criticality Codes	83
<b>Appendix 3</b>	<b>85</b>
Escapes / Diving Catches	85
<b>Appendix 4</b>	<b>88</b>
Human Factors: Additional Information	88
<b>Appendix 5</b>	<b>103</b>
Hydraulics: Additional Information	103
<b>Appendix 6</b>	<b>104</b>

## SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT

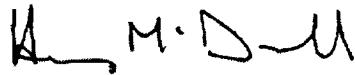
---

Hypergols and Auxiliary Power Unit: Additional Information	104
<b>Appendix 7</b>	<b>105</b>
Propulsion: Additional Information	105
<b>Appendix 8</b>	<b>109</b>
Risk Assessment & Management: Additional Information	109
<b>Appendix 9</b>	<b>110</b>
Software: Additional Information	110
<b>Appendix 10</b>	<b>116</b>
Aerospace Safety Advisory Panel (ASAP) Findings: 1989 to 1998	116
<b>Appendix 11</b>	<b>119</b>
Historical Trends	119
<b>Appendix 12</b>	<b>121</b>
SIAT Members: Backgrounds	121
<b>Appendix 13</b>	<b>126</b>
Historical Shuttle Flight Manifest	126
<b>Appendix 14</b>	<b>127</b>
Orbiter Zones	127
<b>Appendix 15</b>	<b>129</b>
Space Shuttle Hardware Flow	129
<b>Appendix 16</b>	<b>130</b>
Acronyms & Glossary	130
<b>Section 7 - References</b>	<b>133</b>

---

---

## Independent Assessment Team Members



Henry McDonald (*Chair*)

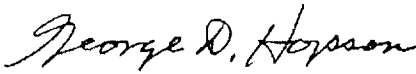
February 9, 2000



Donald Eaton, RADM, USN (Retired)



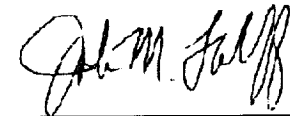
Robert Ernst



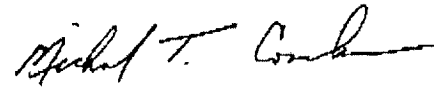
George Hopson



Barbara Kanki



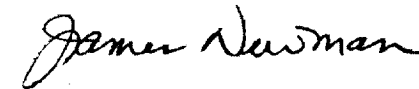
John Lahoff, Lt. Col., USAF



Michael Conahan<sup>1</sup>



John McKeown



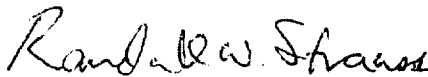
James Newman



Robert Sackheim



George Slenski



Randall Strauss, Col., USAF



John Young

---

<sup>1</sup> Mr. Conahan acted as an independent consultant to the U.S. Government.

## Acknowledgements

Throughout the entire process, the SIAT received the complete support of the Shuttle community. The SIAT was continually impressed with the skill, dedication, commitment and concern for astronaut safety, of the entire Shuttle workforce. The Space Shuttle Independent Assessment Team (SIAT) thanks the technical and management teams of the **Space Shuttle Program Office (SSP), Johnson Space Center, Kennedy Space Center, and Marshall Space Flight Center**, and their supporting contractor organizations.

The SIAT also thanks **Major General Francis C. Gideon, Jr., USAF** and **Major Tracy Dillinger, USAF** from the United States Air Force Safety Center Headquarters, Kirtland AFB for their unwavering support .

Several persons assisted the SIAT as technical contributors, providing their time to gather information that the SIAT further refined. They are listed below.

Our special thanks to Tina Panontin and Luis Mederos. They were a resource for the whole team throughout the process, and worked diligently to integrate this report. This effort would not have been possible without their participation.

## Support Staff

	<u>Affiliation</u>
Luis Mederos ( <i>Executive Secretary to the SIAT</i> )	NASA Ames Research Center
Tina Panontin, PhD, P.E.	NASA Ames Research Center
John Cavolowsky, PhD	NASA Ames Research Center

## Technical Contributors

Multiple personnel provided assistance to the SIAT in the technical areas. The SIAT gratefully acknowledges their assistance.

**Table 1 -- Technical Contributors**

<u>Technical Section</u>	<u>Contributor</u>	<u>Affiliation</u>
Avionics	David Johnson	Wright-Patterson AFB
	David Keyser	Naval Air Systems Command
	Kathy Meesakul	NASA Kennedy Space Center
Human Factors	Barbara Kanki, PhD	NASA Ames Research Center
	Major Tracy Dillinger	USAF HQ Safety Center
	Donna Blankmann-Alexander	United Space Alliance/KSC
	David Driscoll	US Airways
	David Marx	Northwest Airlines
	Jay Neubauer, Lt. Col.	USAF HQ Safety Center
	Duncan Parker	United Space Alliance/KSC
	Cheryl Quinn	NASA Ames Research Center
	William Rankin, PhD	Boeing Company
Hydraulics	James Taylor, PhD	Santa Clara University
	Andreas Dibbern	NASA Kennedy Space Center
	Chris Frissora	Federal Express
Hypergols and Auxiliary Power Unit	Paul Koenig	USAF B2 Program
	Andreas Dibbern	NASA Kennedy Space Center
	Tom Ambrose	NASA DFRC
	Mickey Marianetti	Lockheed Martin Titan 4-B
	Larry Biscayart	NASA DFRC
	Todd Cambell	NASA Kennedy Space Center



**SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT**

---

Problem Reporting & Tracking Process	Tina Panontin, PhD, PE Ann Patterson-Hine, PhD Susan Ahrens John McPherson	NASA Ames Research Center NASA Ames Research Center United Space Alliance/JSC Hernandez Engineering/MSFC
Propulsion	Robert Sackheim George Hopson Lt. Col. John Lahoff	NASA Marshall Space Flight Center NASA Marshall Space Flight Center USAF HQ Safety Center
Risk Assessment & Management	Fayssal Safie, PhD Robert Ernst Prince Kalia Richard Pugh	NASA HQ Naval Air Systems Command United Space Alliance Pratt & Whitney
Safety and Mission Assurance	Tina Panontin, PhD	NASA Ames Research Center
Software	Ann Patterson-Hine, PhD John Bradbury Don Higbee William Jackson Darryl May	NASA Ames Research Center Averstar Averstar NASA Ames Research Center IV&V NASA Johnson Space Center
Structures	James Newman, Jr., PhD Ulf Goranson, PhD Joseph Gallagher, PhD	NASA Langley Research Center Boeing Company University of Dayton
Wiring	George Slenski Ken Christensen Michael Conahan Donald Eaton Robert Ernst Gordon Grooms	Wright-Patterson AFB NASA Ames Research Center Boeing Commercial Naval Postgraduate School Naval Air Systems Command NASA Kennedy Space Center

## Section 1 - Executive Summary

The Shuttle program is one of the most complex engineering activities undertaken anywhere in the world at the present time. The Space Shuttle Independent Assessment Team (SIAT) was chartered in September 1999 by NASA to provide an independent review of the Space Shuttle sub-systems and maintenance practices. During the period from October through December 1999, the team led by Dr. McDonald and comprised of NASA, contractor, and DOD experts reviewed NASA practices, Space Shuttle anomalies, as well as civilian and military aerospace experience.

In performing the review, much of a very positive nature was observed by the SIAT, not the least of which was the skill and dedication of the workforce. It is in the unfortunate nature of this type of review that the very positive elements are either not mentioned or dwelt upon. This very complex program has undergone a massive change in structure in the last few years with the transition to a slimmed down, contractor-run operation, the Shuttle Flight Operations Contract (SFOC). This has been accomplished with significant cost savings and without a major incident. This report has identified significant problems that must be addressed to maintain an effective program. These problems are described in each of the Issues, Findings or Observations summarized below, and unless noted, appear to be systemic in nature and not confined to any one Shuttle sub-system or element. Specifics are given in the body of the report, along with recommendations to improve the present systems.

---

### Issue 1

**NASA must support the Space Shuttle Program with the resources and staffing necessary to prevent the erosion of flight-safety critical processes.**

Human rated space transportation implies significant inherent risk. Over the course of the Shuttle Program, now nearing its 20<sup>th</sup> year, processes, procedures and training have continuously been improved and implemented to make the system safer. The SIAT has a major concern, reflected in nearly all of the subsequent "Issues", that this critical feature of the Shuttle Program is being eroded. Although the reasons for this erosion are varied, it appears to the SIAT that a major common factor among them is the reduction in allocated resources and appropriate staff that ensure these critical processes and procedures are being rigorously implemented and continually improved.

The SIAT feels strongly that workforce augmentation must be realized principally with NASA personnel rather than with contract personnel. The findings show that there are important technical areas that are staffed "one-deep". The SSP should assess not only the quantity of personnel needed to maintain and operate the Shuttle at anticipated future flight rates, but also the quality of the workforce required in terms of experience and special skills. In the recent fleet wiring investigation, work force skill shortages created the need to use Quality Assurance personnel inexperienced in wiring issues to perform critical inspections. Note that increasing the work force carries risk with it until the added work force acquires the necessary experience.

## Issue 2

The past success of the Shuttle program does not preclude the existence of problems in processes and procedures that could be significantly improved.

The SIAT believes that another factor in the erosion referred to in Issue 1 is success-engendered safety optimism. The SIAT noted several examples of what could be termed an inappropriate level of comfort with certain apparently successful "acceptance of risk" decisions made by the program. One example was the number of flights with pinned liquid oxygen injectors flown without prior hot-fire testing that did not experience pin ejection before the STS-93 pin ejection rupture incident. These successful flights created a false sense of security that pinning an injector could be treated as a standard repair. There were 19 incidences of pin ejection that did not result in nozzle rupture prior to STS-93 and this created an environment that led to the acceptance of risk. Similarly the wire damage that led to the short on STS-93 is suspected to have been caused 4 to 5 years prior to the flight. The SSP must rigorously guard against the tendency to accept risk solely because of prior success.

---

## Issue 3

The SSP's risk management strategy and methods must be commensurate with the 'one strike and you are out' environment of Shuttle operations.

While the Shuttle has a very extensive Risk Management process, the SIAT was very concerned with what it perceived as Risk Management process erosion created by the desire to reduce costs. This is inappropriate in an area that the SIAT believes should be under continuous examination for improvement in effectiveness with cost reduction being secondary. Specific SIAT findings address concerns such as: moving from NASA oversight to insight; increasing implementation of self-inspection; reducing Safety and Mission Assurance functions and personnel; managing risk by relying on system redundancy and abort modes; and the use of only rudimentary trending and qualitative risk assessment techniques. It seemed clear to the SIAT that oversight processes of considerable value, including Safety and Mission Assurance, and Quality Assurance, have been diluted or removed from the program. The SIAT feels strongly that NASA Safety and Mission Assurance should be restored to the process in its previous role of an independent oversight body, and not be simply a "safety auditor." The SIAT also believes that the Aerospace Safety Advisory Panel membership should turnover more frequently to ensure an independent perspective. Technologies of significant potential use for enhancing Shuttle safety are rapidly advancing and require expert representation on the Aerospace Safety Advisory Panel. While system redundancy is a very sound element of the program, it should not be relied upon as a primary risk management strategy; more consideration should be given to risk understanding, minimization and avoidance. It was noted by the SIAT that as a result of choices made during the original design, system redundancy had been compromised in 76 regions of the Orbiter (300+ different circuits, including 6 regions in which if wiring integrity was lost in the region, all three main engines would shut down). These were design choices made based on the technology and risk acceptance at that time. Some of these losses of redundancy may be unavoidable; others may not be. In either case, the program must thoroughly understand how loss of system redundancy impacts vehicle safety.

---

## Issue 4

SSP maintenance and operations must recognize that the Shuttle is not an 'operational' vehicle in the usual meaning of the term.

Most aircraft are described as being "operational" after a very extensive flight test program involving hundreds of flights. The Space Shuttle fleet has only now achieved one hundred flights and clearly cannot be thought of as being "operational" in the usual sense. Extensive maintenance, major amounts of "touch labor" and a high degree of skill and expertise by significant numbers of technician and engineering staff will be always required to support Shuttle operations. Touch labor always creates a potential for collateral and inadvertent damage. In spite of the clear mandate from NASA that neither schedule nor cost should ever be allowed to compromise safety, the workforce has received a conflicting message due to the emphasis on achieving cost and staff reductions, and the pressures placed on increasing scheduled flights as a result of the Space Station. Findings of concern to the SIAT include: the increase in standard repairs and fair wear and tear allowances; the use of technician and engineering "pools" rather than specialties; a potential complacency in problem reporting and investigation; and the move toward structural repair manuals as used in the airline industry that allow technicians to decide and implement repairs without engineering oversight. The latter practice has been implicated in a number of incidents that have occurred outside of NASA (Managing the Risks of Organizational Accidents, Chapter 2, p. 21). When taken together these strategies have allowed a significant reduction in the workforce directly involved in Shuttle maintenance. When viewed as an experimental / developmental vehicle with a "one strike and you are out" philosophy, the actions above seem ill advised.

---

## Issue 5

The SSP should adhere to a 'fly what you test / test what you fly' methodology.

While the "fly what you test / test what you fly" methodology was adopted by the Shuttle Program as a general operational philosophy, this issue arose specifically with the Space Shuttle Main Engine (SSME). For the SSME, fleet leader and hot-fire (green-run) testing are used very effectively to manage risk. However, the concept must be rigorously adhered to. Recent experience, for instance the pin ejection problem, has shown a breakdown of the process. An excellent concept, the fleet leader is also applicable to other systems, but its limitations must be clearly understood. In some cases (e.g., hydraulic testing, avionics, Auxiliary Power Unit) the SIAT believes that the testing is not sufficiently realistic to estimate safe life.

## Issue 6

The SSP should systematically evaluate and eliminate all potential human single point failures.

In the past, the Shuttle Program had a very extensive Quality Assurance program. The reduction of the quality assurance activity ("second set of eyes") and of the Safety & Mission Assurance function ("independent, selective third set of eyes") increases the risk of human single point failures. The widespread elimination of Government Mandatory Inspection Points, even though the reductions were made predominantly when redundant inspections or tests existed, removed a layer of defense against maintenance errors. Human errors in judgment and in complying with reporting requirements (e.g., in or out of family) and procedures (e.g., identification of criticality level) can allow problems to go undetected, unreported or reported without sufficient accuracy and emphasis, with obvious attendant risk. Procedures and processes that rely predominantly on qualitative judgements should be redesigned to utilize quantitative measures wherever possible. The SIAT believes that NASA staff (including engineering staff) should be restored into the system for an independent assessment and correction of all potential single point failures (see also the concerns concerning the Safety and Mission Assurance function in **Issue 3**).

---

## Issue 7

The SSP should work to minimize the turbulence in the work environment and its effects on the workforce.

Findings support the view that the significant number of changes experienced by the Shuttle Program in recent years have adversely affected workforce morale or diverted workforce attention. These include the change to Space Flight Operations Contract, the reduction in staffing levels to meet Zero Based Review requirements, attrition through retirement, and numerous re-organizations. Ongoing turbulence from cyclically heavy workloads and continuous improvement initiatives (however beneficial) were also observed to stress the workforce. While the high level workforce performance required by the Shuttle program has always created some level of workforce stress, the workforce perception is that this has increased significantly in the last few years. Specifically, the physical strain measured in the Marshall Space Flight Center workforce significantly exceeded the national norm, whereas the job stress components (e.g., responsibility levels, physical environment) were near normal levels. This typically indicates the workforce is internalizing chronic instability in the workplace. Similarly, feedback from small focus groups at Kennedy Space Center indicates unfavorable views of communication and other factors of the work environment. Clearly, from a health perspective, one would seek to reduce employee stress factors as much as possible. From a vehicle health perspective, stressed employees are more likely to make errors by being distracted while on the job, and to be absent from the job (along with their experience) as a result of health problems.

The SIAT believes that the findings reported here in the area of work force issues parallel those that were noted by the Aerospace Safety Advisory Panel. The SIAT is concerned that in spite of the Aerospace Safety Advisory Panel findings and recommendations, supported by the present review, these problems remain.

## Issue 8

The size and complexity of the Shuttle system and of the NASA/contractor relationships place extreme importance on understanding, communication, and information handling.

In spite of NASA's clear statement mandate on the priority of safety, the nature of the contractual relationship promotes conflicting goals for the contractor (e.g., cost vs. safety). NASA must minimize such conflicts. To adequately manage such conflicts, NASA must completely understand the risk assumptions being made by the contractor workforce. Furthermore, the SIAT observed issues within the Program in the communication from supervisors downward to workers regarding priorities and changing work environments. Communication of problems and concerns upward to the SSP from the "floor" also appeared to leave room for improvement. Information flow from outside the program (i.e., Titan program, Federal Aviation Administration, ATA, etc.) appeared to rely on individual initiative rather than formal process or program requirements. Deficiencies in problem and waiver tracking systems, "paper" communication of work orders, and FMEA/CIL revisions were also apparent. The program must revise, improve and institutionalize the entire program communication process; current program culture is too insular in this respect.

Additionally, major programs and enterprises within NASA must rigorously develop and communicate requirements and coordinate changes across organizations, particularly as one program relies upon another (e.g., re-supplying and refueling of International Space Station by Space Shuttle). While there is a joint Program Review Change Board (PRCB) to do this, for instance on Shuttle and Space Station, it was a concern of the SIAT that this communication was ineffective in certain areas.

---

## Issue 9

Due to the limitations in time and resources, the SIAT could not investigate some Shuttle systems and/or processes in depth.

Follow-on efforts by some independent group may be required to examine these areas (e.g., other propulsion elements, such as the Reusable Solid Rocket Motor, Solid Rocket Booster, External Tank, Orbiter Maneuvering System, and Reaction Control System, and other wiring elements besides those in the Orbiter). This independent group should also review the SSP disposition of the SIAT findings and recommendations.

The Shuttle Upgrades program creates the opportunity to correct many of the observed deficiencies, e.g., the 76 areas of compromised redundancies (300+ circuits), and to incorporate design for maintainability and continuous improvement. However, without careful systems integration and prioritization, some of the deficiencies observed by the SIAT will be exacerbated, e.g., in wiring, hydraulics, software, and maintenance areas. Additionally, the elements of maintenance must be rigorously analyzed, including training, maintainability, spares support maintenance, and accessibility.

## Return To Flight

The SIAT was asked by the SSP for its views on the return to flight of STS-103. The SIAT had earlier considered this question and had concluded that a suitable criterion would be that STS-103 should possess less risk than, for example, STS-93. In view of the extensive wiring investigation, repairs and inspections that had occurred this condition appeared to have been satisfied. Furthermore, none of the main engines scheduled to fly have pinned Main Injector liquid oxygen posts. The SIAT did suggest that prior to the next flight the SSP make a quantitative assessment of the success of the visual wiring inspection process. In addition, the SIAT recommended that the SSP pay particular attention to inspecting the 76 areas of local loss of redundancy and carefully examine the OV102 being overhauled at Palmdale for wiring damage in areas that were inaccessible on OV103. Finally, the team suggested that the SSP review in detail the list of outstanding waivers and exceptions that have been granted for OV103. The SSP is in the process of following these specific recommendations and so far has not reported any findings that would cause the SIAT to change its views.

Shortly before completing this report, the SIAT was gratified to learn that a number of steps had been taken by NASA to rectify a number of the adverse findings reported above. Of particular note was the strengthening of the NASA Quality Assurance function for the Shuttle at Kennedy Space Center. Upon completion of STS-103, the SIAT was pleased to learn that only two orbiter in-flight anomalies were experienced, a reduction from past trends (see **Appendix 11**).

---

## **Section 2 - Charter**

---

### **Guidance from Associate Administrator**

The charter from the Associate Administrator for Space Flight, Mr. Joseph Rothenberg, to the Independent Assessment Team on September 7, 1999 is as follows:

"Dr. McDonald will lead an Independent Technical Team to review the Space Shuttle systems and maintenance practices. The Team will be comprised of NASA, contractor, and DOD personnel and will look at NASA practices, Shuttle anomalies, and civilian and military experience."



## Section 3 - Introduction

During the launch of STS-93 in July, 1999, two serious in-flight anomalies occurred. The first occurred five seconds after lift-off when a primary and back-up main engine controller on separate engines dropped offline due to a power fluctuation. Post-flight inspection revealed a single 14 ga. polyimide wire had arced to a burred screw head. The second anomaly was a liquid oxygen low-level cutoff 0.15 seconds before the planned Main Engine Cut Off (MECO). Post flight inspection of the affected engine indicated that a liquid oxygen post pin had been ejected and had penetrated three nozzle coolant tubes, causing a fuel leak and premature engine shut-off. On a previous flight, STS-95/OV103, the drag chute door released prematurely about 2 seconds after main engine ignition during liftoff. Still another incident occurred on the ferry flight of OV102 to Palmdale, for which washers on several attachment bolts were not installed. System design and redundancy successfully handled each anomaly and allowed safe flight of the vehicle and mission completion. However, the occurrence of the anomalies raised concerns over the adequacy of Shuttle operations and maintenance procedures, particularly in light of the age and projected extended life (to the year 2010) of the Shuttle.

The Shuttle Independent Assessment Team (SIAT) was formed by Dr. Henry McDonald, Director of NASA Ames Research Center, at the request of the Associate Administrator for Space Flight, Mr. Joseph Rothenberg. Comprised of members from NASA, industry, academia, and the military, the SIAT possessed a broad and relevant experience base, which included the problems arising from downsizing and outsourcing of maintenance depots, as well as specific expertise, e.g., in the problems of wiring in aging aircraft. The SIAT's charter was to bring to Shuttle maintenance and operations processes a perspective from the best practices of the external aviation community, and report to the Associate Administrator (Office of Space Flight) in approximately 60 days. The SIAT began its work on October 4, 1999, and signed off on the final report by February 9, 2000; the present report summarizes its activities.

The assessment was organized around the four potential sources of failures in complex engineering systems<sup>1</sup>, as shown schematically below.

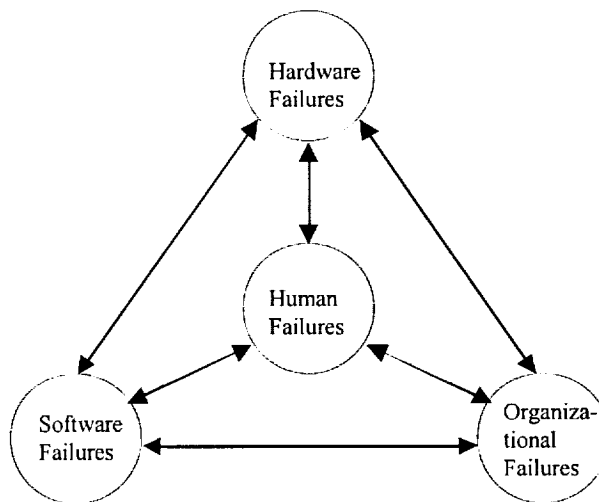


Figure 1 -- System Failure Sources

To assess potential sources of hardware anomalies, reviews were made of major Shuttle systems including: avionics, hydraulics, hypergols and Auxiliary Power Units (APU's), propulsion, structures, and wiring. The Shuttle electrical wiring system was an area of particular interest, as recent experience on STS-93 had given an indication that a previously unrecognized systemic problem may exist. In the area of software, validation and verification of both ground and flight software were examined. Human factors were investigated in maintenance, operations, and engineering workforces. Organizational or process issues included risk assessment and management, problem reporting, and the Safety and Mission Assurance function. The interdependencies between the potential sources of failures were considered in each case, with particular attention to identifying procedures or processes in which human failure by a single individual could cause loss of vehicle and/or mission (i.e., human single point failures). Time restricted the review to the Shuttle Orbiter, principally. However, it is felt that many of the same issues could potentially arise with other components of the Space Transportation System.

Observations and findings were generated from information provided in formal, detailed briefings to the SIAT by the Space Shuttle Program (SSP) staff and contractors. The discussion was allowed to follow any direction believed to be important by the SIAT within the general framework of the charter. Additional information was provided by domain experts who functioned as consulting advisors to the SIAT in the review of the specialized areas listed above. The team made five site visits (see Table 2 -- Meeting Dates and Locations), with a final review meeting held in December at Kennedy Space Center immediately prior to the flight of STS-103. The domain expert consultants made additional site visits in support of the SIAT activities. The SIAT also benefited from discussions with members of the Aerospace Safety Advisory Panel (ASAP), The Titan IV Accident Review Team, and a Lockheed-Martin internal review team led by Mr. Thomas Young. The SIAT believes that significant areas of similarities exist between the findings of these various reviews.

Table 2 -- Meeting Dates and Locations

<b><u>Event</u></b>	<b><u>Dates</u></b>	<b><u>Location</u></b>
Meeting #1	Oct. 4-5, 1999	NASA Ames Research Center (Mountain View, CA)
Meeting #2	Oct. 14-15, 1999	Palmdale Facility (Palmdale, CA)
Meeting #3	Oct. 21-22, 1999	NASA Kennedy Space Center, FL
Meeting #4	Oct. 28-29, 1999	NASA HQ (Washington, DC)
Meeting #5	Nov. 8-9, 1999	NASA Johnson Space Center (Houston, TX)
Meeting #6	Dec. 9-10, 1999	NASA Kennedy Space Center, FL

Recommendations were generated for immediate, intermediate, and long-term improvements or solutions to identified concerns. In a number of cases, the recommendations were for NASA to institute more detailed exploration as a possible problem area required much more time and effort to ascertain its existence or depth than the SIAT could undertake. The following sections of the report discuss specific findings and recommendations made for each of the areas named above. Appendices contain additional background materials for some of these technical sections.

## Section 4 - Technical Sections

The following technical sections cover specific systems of the Shuttle and processes of Shuttle operations and maintenance that were reviewed during the course of the independent assessment.

---

### Technical Section Listing

- Avionics
- Human Factors
- Hydraulics
- Hypergols and Auxiliary Power Unit
- Problem Reporting & Tracking Process
- Propulsion
- Risk Assessment & Management
- Safety and Mission Assurance
- Software
- Structures
- Wiring

## Avionics

### Findings

1. Conversion from the Launch Processing System to the Checkout & Launch Control System and the number of scheduled launches suggests a risk of work overload and high stress for the personnel responsible for ground processing of Orbiter systems.
2. The operability of flight equipment spares, piece part spares, and test equipment, all subjected to long periods of storage without operation or testing, is not being evaluated. Certain older component technology families are known to be subject to degradation even under benign storage conditions.
3. An aggressive program to assess and manage critical avionics component obsolescence is absent.
4. NASA Shuttle Logistics Depot data suggest that maintenance documentation packages obtained when a Line Replaceable Unit is transitioned to NASA Shuttle Logistics Depot are not always complete. Old and aging Line Replaceable Units that have not had much maintenance may have missing documentation that over time becomes unavailable.
5. There is a need to make the maintenance databases more user-friendly and complete (see **Problem Reporting & Tracking Process**).
6. There is excessive use of waivers and declaring of events as unexplained anomalies to return equipment to flight status. This increases the probability of more failures during launch preparation and on orbit. These practices are of greatest concern when CRIT 1 (see **Appendix 2**) signal paths are involved.
7. Limited test capability, documentation, and experience has forced reliance on the Line Replaceable Unit as a test fixture, limiting identification of root cause failure and causing excessive and undocumented wear.
8. The contractor's avionics repair facility lacks up-to-date automatic test equipment, tracking of failure rates and causes, and expert systems used in industry to aid in trouble shooting. Furthermore, the avionics facility lacks sufficient environmental control, insulated safety mats at work stations and emergency electrical power shut-off in the event of technician distress.

### Recommendations

1. A formal Aging and Surveillance Program should be instituted.
2. The SIAT recommends an evaluation of depot repair documentation be performed to determine if the transition process attained a necessary and sufficient set of vendors for each Line Replaceable Unit, Shop Replaceable Unit, and special test equipment.
3. All testing of units must be minimized and documented as part of their total useful life. Similarly, maintenance operations must be fully documented.
4. The failure of all CRIT 1 units should be fully investigated and corrected without waivers.
5. The avionics repair facility should be brought up to industry standards.
6. NASA and USA quality inspection and NASA engineers should review all CRIT 1 system repairs.
7. NASA should expand existing data exchange and teaming efforts with other governmental agencies especially concerning age effects.
8. Standard repairs on CRIT1 components should be completely documented and entered in the Problem Resolution and Corrective Action system.

- 
9. The criteria for and the tracking of standard repairs, fair wear and tear issues, and their respective FMEA/CIL's should be re-examined.
  10. The SIAT recommends comprehensive re-examination of maintenance and repair actions for adequate verification requirements (e.g., visual, proof test, or green run).
  11. Where redundancy is used to mitigate risk, it should be fully and carefully implemented and verified. If it cannot be fully implemented due to design constraints, other methods of risk mitigation must be utilized.

## Introduction

The SIAT's objective was to identify topics within the avionics maintenance processes and procedures that may require more detailed evaluation and possible corrective actions. The scope of the task was to evaluate maintenance processes and procedures for the avionics suite aboard the Orbiters and solid rocket boosters. The maintenance history, processes, and procedures for two avionics systems or sub-systems with high criticality and high complexity/performance characteristics were to be selected for evaluation.

The steps taken to accomplish the objectives were:

1. Review of Shuttle avionics suite architecture
2. Review of Orbiter Processing Facility, NASA Logistics, and NASA Shuttle Logistics Depot maintenance processes and procedures
3. Review of maintenance data and available data bases
4. Interviews with NASA and USA personnel
  - at Kennedy Space Center (Orbiter system engineers, logistics engineers, Orbiter Processing Facility technicians)
  - at NASA Shuttle Logistics Depot (logistics engineer, avionics repair engineers and technicians, configuration control engineers, work control personnel, among others)
5. Site visit to NASA Shuttle Logistics Depot
  - Step-by-step Line Replaceable Unit handling and repair flow from incoming/receiving to shipping
  - repair work stations
  - test equipment
  - case files
6. Documentation control and reproduction

A list of the top 30 avionics Line Replaceable Units with the greatest maintenance demand was provided by NASA Shuttle Logistics Depot. This was used to identify the Ku band Line Replaceable Units and multiplexer/demultiplexer (MDM) units for more detailed evaluation. The Test, Teardown and Evaluation Corrective Action Record reports for the Ku band equipment and the MDM units covering the last three years were received at the Air Force Research Laboratories for review.

The NASA Shuttle Logistics Depot is apparently certified to repair about 70% of the Orbiter and Solid Rocket Booster avionics. The remaining 30% are maintained by the original vendor or a third party. However, time did not permit evaluation of vendor or third party maintenance processes and procedures.

Some key maintenance data was not available during the Kennedy Space Center and the NASA Shuttle Logistics Depot site visits. Therefore, DOD technical contributors conducted individual evaluation tasks guided by experience with commercial and military avionics maintenance operations, with the military Titan missile, and with logistics support of both NASA and USAF space programs. However, follow-on efforts may be needed.

---

## Assessment

No specific or systemic problems were discovered during performance of the avionics maintenance subtask that were judged to be a direct risk to safety of flight. However, the conversion from the Launch Processing System to the Checkout & Launch Control System could pose an indirect risk if not appropriately managed.

The addition of Checkout & Launch Control System requirements writing and software/hardware verification are adding significantly to the workload of these systems engineers. Some have been working substantially more than 8 hours per day during this past year with only two scheduled launches. There is considerable doubt that the systems engineers will be able to sustain the work load inherent in pre-launch preparation for the anticipated 2000 year level of 8 Shuttle missions while writing Checkout & Launch Control System requirements and validating/certifying the new Checkout & Launch Control System software and hardware. When performing some tests on the current Launch Processing System, the engineer is presented values on video monitors, which must be accurately compared with written limits. The engineer must identify a failed test. Work overload raises a concern about errors during Shuttle pre-launch system. Currently the downstream checks will most likely catch these errors should they pose a safety of flight concern. Any such errors however are significantly more difficult to repair the later in the flow they are uncovered. It is recommended that further evaluation of this workload issue be performed and the Checkout & Launch Control System schedule appropriately adjusted to control workload.

Several technical concerns are recommended for further evaluation. These are likely to cause future problems with cost or timeliness of avionics repairs and could adversely affect the mission capability and readiness of the Shuttle fleet.

Spare parts, assemblies, and Line Replaceable Units are kept in long-term storage. The following questions arise from this practice: Are these items now in usable condition? Will they remain suitable for use indefinitely?

No inventory monitoring process is in place to evaluate degradation or failure of most items stored as spares for long periods. There are known problems with some older discrete (transistors, diodes, etc.) and microcircuits (monolithic, multichip and hybrid ICs) semiconductor families, which can cause degradation or failure. MIL-M-38510, the general specification for microcircuit semiconductor devices, had requirements for periodic solderability testing and 100% screening of all electrical characteristics. These periodic tests and screens were required if devices were held in long term storage. There was a demonstrated need for this testing. The purpose was to ensure parts had not degraded or failed while in storage. Other component types (e.g., capacitors, and carbon composition resistors) are also susceptible to degradation during long term storage. These problems affect unused parts, as well as, those already used in circuit assemblies. It is recommended that the condition of stored parts, assemblies, and Line Replaceable Units be evaluated to determine the serviceability and the flight worthiness of spare Line Replaceable Units.

Both Space Shuttle avionics equipment and spare assemblies were built with many parts that are no longer available from any source. While a lifetime supply has been acquired, the quality of the parts in long term storage is questionable. Many may be degraded to a degree that several must be tried before one is found that works properly. Those spares that do initially work may fail at a shorter than expected interval. Therefore, spares inventory may not provide as long a period of support as the number of units in the bins might suggest. Suitable replacements are often costly and time consuming to find and qualify. It is recommended that an evaluation of parts obsolescence be performed. It should include evaluation of the quality of various spare part types in long term storage. This is likely to be a significant problem when the flight rate increases.

Parts obsolescence may also be a problem of unrecognized magnitude with respect to test equipment the NASA Shuttle Logistics Depot keeps in long-term storage. The SIAT was told that there are some Line Replaceable Units that the NASA Shuttle Logistics Depot is certified to repair that have not failed since the NASA Shuttle Logistics Depot became the certified depot. There are testers that have been in storage for more than ten years. Until such equipment is needed, it is left in warehouse storage untouched. The operability of any electronic equipment built with early generations of semiconductors and moisture sensitive components is uncertain. Many of the parts needed to repair test equipment more than ten or fifteen years old are no longer available from either the test equipment or part vendors. The NASA Shuttle Logistics Depot apparently does not have a spare parts inventory for the special test equipment in long term storage. A significant risk exists that parts obsolescence will

---

render this equipment unrepairable when it is eventually needed. It is recommended that the operability and reparability of Special Test Equipment in long term storage be evaluated.

There have been hundreds of requests for repair documents that were found to be unavailable in the maintenance document library even though the NASA Shuttle Logistics Depot was certified to perform the repair that prompted the requests. These necessary vendor documents were missed during the depot transition process. Most of these documents were requested because they were necessary to enable specific diagnostics and repairs. The need for them was identified because a certain failure had occurred. Not having some of these documents could cause work stoppages. Since a significant number of Line Replaceable Units apparently have had few or no repairs since the NASA Shuttle Logistics Depot certification, it is reasonable to presume there remains a very large number of documents that have not yet been determined to be "missing".

Aging will eventually cause an increased demand for maintenance on virtually all Line Replaceable Unit and Shop Replaceable Unit assemblies. However, since this equipment has been out of production and has not required much maintenance, the associated documentation may no longer be available from any source. In addition, the NASA Shuttle Logistics Depot data suggests that the price being asked for some old maintenance documentation may be excessive. Unavailable maintenance data will increase the need for costly and time consuming circuit analysis and cause very long repair cycle times. It is recommended that an evaluation of available maintenance and design related data be performed for Line Replaceable Units that have so far required little, or no maintenance, but will eventually.

SIAT member experience with maintenance practices, as well as, failure and root cause analyses, suggests the number of Problem Reports being closed by wavier or declared to be unexplained anomalies is a concern. In discussions with members of the Shuttle maintenance community it was mentioned that very little money was available to perform detailed failure analyses and that once the money for the year was gone, no additional failure analyses were possible. Not pursuing pattern failures in highly critical equipment can certainly increase the risk of a lost mission and can also increase the maintenance burden and support costs. An independent review of policies and procedures related to closing Problem Reports by wavier or as unexplained anomalies is recommended. This same issue has appeared in a number of other areas.

One or two records reviewed, as a part of this study did not appear to be technically defensible. In one case, merely monitoring the output frequency of an oscillator, as it ran for a period of time while exposed to fairly moderate temperature cycling, was identified as the means by which the circuit repair had been performed. Apparently, as soon as the output was observed to have drifted within limits, the circuit was declared fixed. There was no identification of root cause and therefore no real repair was possible. It is recommended that a review of maintenance records be performed to ensure that repair actions are reasonable and appropriate for the indications of failure and diagnostic results. Such a review should be part of the wider review recommended in **Issue 9**.

During the avionics maintenance subtask effort, various requests for trend and summary maintenance data were made. It appeared that considerable effort would be required to obtain the data. The decision had to be made to drop some data requests since the study was scheduled to end before it could be made available. The SIAT members believe there is a needed for improvements to maintenance data bases so very old avionics equipment can be maintained in safe operating condition. Timely access to good data can save time, money and support better first pass success with repairs. The SIAT recommends that the adequacy, sufficiency, and ease of use of maintenance databases be evaluated (see **Problem Reporting & Tracking Process**).

## Summary

In the brief period of evaluation available for this review, no problems directly jeopardizing safe flight were identified by the SIAT technical team. Several technical concerns were identified that if left unresolved could seriously affect the cycle time and/or cost of repairs. These concerns are listed in the Findings section and discussed in the Assessment section above.

## Human Factors

### Findings

1. Communication difficulties exist between all parties particularly in accepting feedback from the workforce, Aerospace Safety Advisory Panel, and independent assessment groups. This factor erodes trust and loyalty within the workforce which are essential for safe work practices.
2. Failure to incorporate Human Factors as a critical part of the decision process has increased potential single point and multiple point failures.
3. Recent numerous changes and transitions adversely affect work practices, resulting in loss of technical and process-related corporate knowledge (see **Issue 7**).
4. Process improvements made during the transition period to Shuttle Flight Operations Contract have also brought workforce concerns.
5. Work stresses, including expanded work assignments and diminished team support, have reduced the capabilities of the downsized workforce. Innovative cross training approaches may be key to regaining competencies and taking advantage of the skill and experiences of an aging workforce.
6. The SIAT is concerned that in spite of the Aerospace Safety Advisory Panel recommendations and findings, supported by the SIAT, recurring human factors issues remain unresolved.
7. Employee surveys, although limited in current scope, show significant levels of Physical Strain (internalized chronic stress). Internalized chronic stress has been implicated in workers suffering from stress related disease (e.g., gastrointestinal, cardiac, migraines).

### Recommendations

1. Communications between the rank and file work force, supervisors, engineers and management should be improved.
2. Human error management and development of safety metrics, e.g., Kennedy Space Center Shuttle Processing Human Factors team, should be supported aggressively and implemented program-wide.
3. Selected areas of staffing need to be increased (e.g., the Aerospace Safety Advisory Panel advised 15 critical functional areas are currently staffed one deep).
4. The SIAT recommends that the SSP implement the Aerospace Safety Advisory Panel recommendations. Particular attention should be paid to recurring items.
5. NASA should expand on the Human Factors research initially accomplished by the SIAT and the Air Force Safety Center. This work should be accomplished through a cooperative effort including both NASA and AFSC. The data should be controlled to protect the privacy of those taking the questionnaires and participating in interviews. Since major failures are infrequent occurrences, NASA needs to include escapes and diving catches (see **Appendix 3**) in their human factors assessments.
6. Work teams should be supported through improved employee awareness of stresses and their effect on health and work. Workload and "overtime" pressures should be mitigated by more realistic planning and scheduling; a serious effort to preserve "quality of life" conditions should be made.
7. Teamwork and team support should be enhanced to mitigate some of the negative effects of downsizing and transition to Shuttle Flight Operations Contract. Most immediately needed is the provision of relief from deficits in core competencies, with appropriate attention to the need for experience along with skill



---

certification. Further development of the use of cross-training and other innovative approaches to providing on-the-job training in a timely way should be investigated.

## Introduction

The SIAT gathered information by conducting semi-structured group and individual interviews and reviewing a variety of available documentation. Numerous sources of written documentation exist in concert with the Shuttle program from safety reports and previous assessment efforts. Group interviews occurred at KSC and Palmdale while individual interviews occurred at KSC. In addition, the Occupational Stress Inventory (a psychological test with validated national averages) was to be given at 3 Space Centers. Only one, at Marshall Space Flight Center, was completed in time for this report.

The discussion of the results of the interviews and the Occupational Stress Inventory is followed by additional discussion by the industry technical group assisting the SIAT for Human Factors. This group adopted the goal of identifying the maintenance practices and lessons learned from the aviation industry that pertain most directly to the SIAT human factors concerns; namely those human factors issues related to the causes and contributors to maintenance error, and potential risk to mission safety. Although it was not feasible for the technical group, as a whole, to conduct observational visits to Shuttle operational sites, each of the individuals supporting the SIAT has longstanding, personal experience in coping with the issues of concern. Together, they provide a balance of perspectives from aviation: air carrier operations, manufacturers, government and research. **Appendix 4** contains additional supporting information.

## Assessment

### Group Interviews

Groups were asked to comment and rank from 1-5 their perception of the following 6 categories: 1) Unity, 2) Communication, 3) Justice, 4) Flexibility, 5) Support, and 6) Learning. Requests for this feedback were intentionally worded in an open-ended fashion to exclude positive or negative implications. Participants were informed that their feedback was anonymous, their responses would be used within the SIAT, and there would be no retribution for group participation. The interview results consistently highlighted the role of human factors within the Shuttle organization and show consistent trends -- specifically the negative "people" effects resulting from degraded communication, morale, training, retention, and physical health. These issues cross organizational boundaries and occupational roles: across the approximately 40 individuals from which we received input, approximately 30% were NASA and 70% were contractors representing multiple job classes (NASA Quality assurance, Safety and Engineering, Contractor Quality assurance, Technicians, Team Leads and Supervisors).

The following group responses mirrored individual responses from additional interviews.

1. Unity (knowing the common goal and collaboration to achieve it) was described as degraded due to fewer people, greater uncertainty, increased responsibilities, heightened job insecurity and overall organizational unpredictability.
2. Communication (sending and receiving information Up, Down, and Laterally) was described as poor due to fragmented organizational structure as well as few available modes. Of special concern, fear of retribution for 'speaking out' was expressed with several concrete examples related including the informal punitive status of "three days on the beach". It is important to note that whether this is a current practice or not, it is perceived reality by the workers. Communication "Within" the organization with peers, described as "circling the wagons" (for survival) was rated as good. Concern was expressed regarding previous attempts to address problems ("we told this to the ASAP team") and questions ("is this another bureaucratic exercise?") were voiced. Concern for appearing to "cry wolf" by raising issues in the light of no disastrous outcomes was also expressed.

3. Justice, (knowing the rules, equitable responses to violations, as well as recognition for outstanding performance) was described as unpredictable, capricious and highly dependent on the individual's supervisor.
4. Flexibility (the ability of the organization to rise and meet critical demands and return to "normal operations") was described as poor. Changes in training process, expectations, certification, and oversight of training/certification programs were felt to negatively impact the organizations safety. The example of "creative clears" was offered. This effort to ensure efficiency by modifying safety guidance has at times allowed a greater number of people to be exposed to high risk procedures.
5. Support was described as fair to poor based on lack of modern equipment, and appropriate manning levels. Within group support was felt to be good while support from other agencies (and funding sources) was felt to be detrimental to the space program.
6. Learning was described as poor due to staffing and experience losses, but especially due to the loss of redundancy. The decrease in oversight and inspectors was brought up as well as modifications that result in short-term improvements, but may be short-sighted. For example, to become ISO9000 compliant, informal corporate knowledge (documentation and diagrams) was destroyed in spite of attempts to keep historical records. It is not feasible to reconstruct this information, especially in light of the aging workforce; this was later acknowledged.

### Physical Strain on Staff

Another issue brought up in the groups was emphatically illustrated by the "experienced group" (all over 20 years with the Shuttle program). Four of six people within this group were taking medication for hypertension. They felt the number of their peers who have retired, obtained jobs elsewhere, medically retired, or suffered heart attacks or strokes was very high. The Occupational Stress Inventory (a psychological test with validated national averages) was to be given at three Space Centers. Only one, at Marshall Space Flight Center, was completed in time for this report. The Marshall results fall into the "normal" range of scores with the exception of physical strain. Physical strain is an indicator of chronic stress that has been internalized to the point the workers are suffering from stress related disease. Examples would include gastrointestinal (ulcers), cardiac (heart problems, high blood pressure, stroke), or central nervous system (migraines) problems. These results match the KSC personnel comments that many of their friends have left the workforce due to significant health related problems. Additional testing of other NASA centers may provide insight on the type, extent, and pervasiveness of stress related issues. Climate indicators (see Figure 2) for the KSC workforce<sup>2</sup> of overtime, compensatory time, and employee assistance program visits, support the finding of increasing workforce stress.

Although faced with daunting and frustrating technological, economic and personnel challenges, all personnel expressed a deep commitment to manned space flight, the space program, and the desire to bring a new generation of workers into the SSP fold. They expressed hope that conditions would improve in all areas.

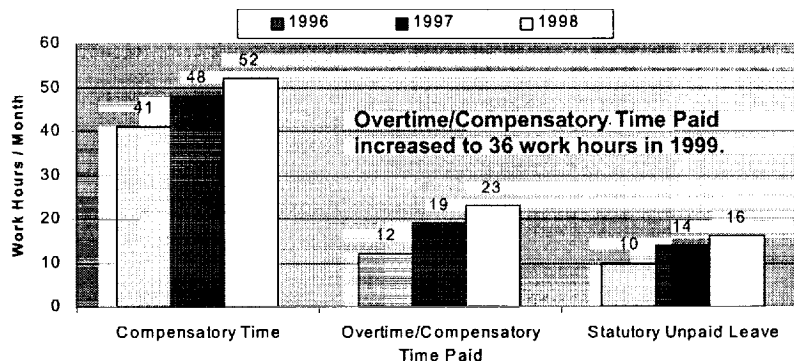


Figure 2 -- Kennedy Space Center Workforce Climate Indicators

## Other Major Areas of Concern

Human factors concerns (see below) represent different types of weaknesses in the defense layers of maintenance activities, not as causal factors that necessarily lead to error. In contrast, building up defenses where weaknesses are identified will reduce the likelihood that "holes" in defenses will line up and result in a maintenance error. In addition to a weakened defense against error, other types of team performance decrements may emerge such as reduced productivity and decreased employee morale. The basic safety model that symbolizes these attributes is commonly known as the "Swiss Cheese" model by James Reason (see Figure 3). In this model, various layers of defenses against human error range from 1) high level decision makers, 2) line management and other support organizations, 3) preconditions for work, 4) the production act itself, and 5) human error defenses to safeguard against hazards

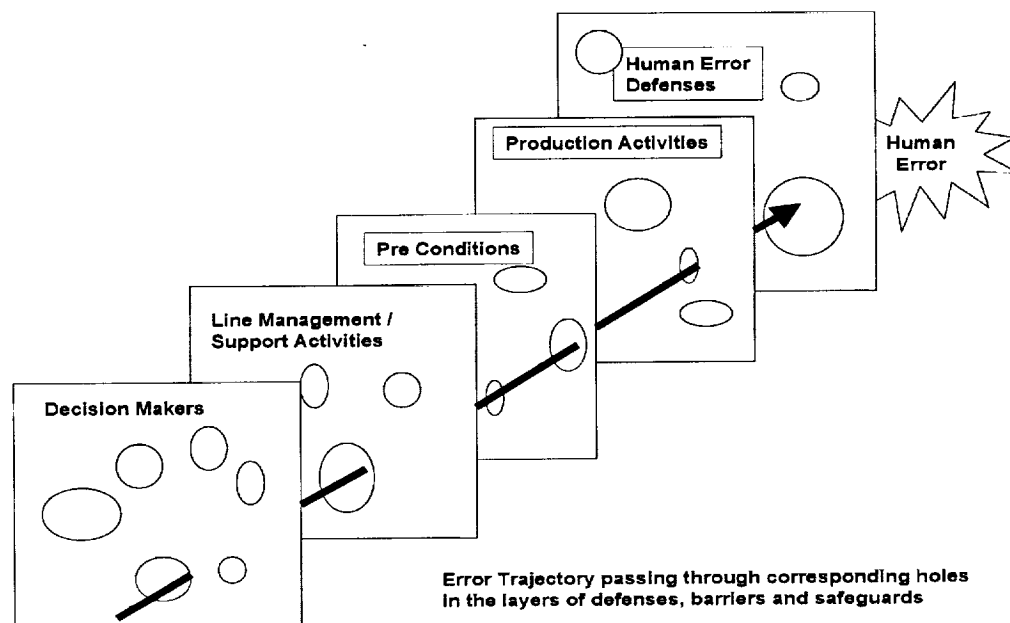


Figure 3 -- Model of Human Error (adapted from J. Reason, 1997)

Four major areas of concern were identified by the technical contributors assisting the SIAT. These are discussed below.

### Communication and Cooperation

A vital element of any Aviation Maintenance Human Factors Program is the issue of management/workforce cooperation. If quality of maintenance performed enhances flight safety, and quality of work results from positive cooperative efforts, then it behooves all parties to exert this effort. Positive attitudes produce positive results.<sup>3</sup> Open and honest communication from workforce to management as well as from management to workforce was observed to be lacking in many areas (see Finding 1). In general, a need for management to communicate and provide feedback to the workforce, and for the workforce to be given greater opportunities to provide input, was observed.

#### Human error management and safety metrics

The Kennedy Space Center Human Factors Integration Office and the Kennedy Space Center Shuttle Processing Human Factors Team should be supported aggressively and provided enough resources so they may address all areas of the program. They have systematically approached event investigations by using the Kennedy Space Center Human Factors Event Evaluation Model. From all industry standards, what the SIAT has seen is an excellent model for identifying root causes and contributing factors in the error event chain. It is particularly effective because it has been thoroughly adapted to the Kennedy Space Center work environment and because it preserves the level of complexity that characterizes error event scenarios. Each of these teams has developed goals and objectives that are admirable, but far exceed their resources.

#### Teamwork and Team Support

Due to the combined effects of downsizing and transition to the Shuttle Flight Operations Contract, the way in which teams used to work changed. Although the Shuttle Processing Human Factors Team had addressed Task Team Leadership at one time, this concept can no longer be applied in the same way. Resources are stretched thin, and there are now situations in which technicians cannot rely on the same resources and infrastructure as before. In the spirit of open and honest communication, many of the negative effects of these changes might have been mitigated if the workforce were more appropriately prepared, retrained and, in some cases, retained. Because people are covering more jobs and more responsibilities and are working across different facilities, the training needs have changed and increased. Workload and hours/per day and week may or may not be different but the availability of resources during those hours has diminished.

In the Lockheed-Martin Titan briefing<sup>4</sup> a parallel issue is observed. Similar to the Shuttle, wiring damage was found to be maintenance induced. In tracking the potential for collateral maintenance damage, cases where technicians could become "single points of failure" were discovered. In such cases, corrective actions required a significant enhancement to team support including: 1) development of a "Buddy System" of monitoring maintenance work, 2) Error prevention training and 3) Development of Denver/Cape Integrated Product Teams for product reviews.

#### Maintenance Process Improvements

Clearly many process improvements were made during the downsizing and transition period. Concerns arise more from timing issues than inadequacies. For instance, if two jobs or shops were to merge, it is critical that the processes be analyzed and improved before the change takes place. In addition, personnel need to be adequately prepared for the change. While diminishing resources are compelling, they cannot become the "excuse" for making process changes. One way to facilitate employee preparation is to involve them in the process. Numerous innovative methods are being developed across other high risk industries; many of these relying heavily on input and feedback from the users. Given the Aerospace Safety Advisory Panel finding that incorrect documentation is often implicated in errors committed, this is a prime area for supporting employee involvement. In addition, the introduction of new technologies (for process improvement) is another prime target for user feedback at every phase of development and implementation. Finally, the general issue of improving safety metrics is relevant in the assessment of all process improvements.

Other areas of concern, including human error management, human factors training, and other process or ergonomic improvements are discussed in **Appendix 4A: Lessons Learned from Aviation**.

## **Summary**

The human factors findings are of great concern to the SIAT and merit greater attention, particularly those that have surfaced repeatedly (e.g., ASAP findings) and those that cause enduring physical strain. Due to the small proportion of personnel involved in the group interviews and surveys, a focused independent inquiry, while beyond the scope of the SIAT, is strongly recommended to clarify these issues and help in developing new timely and program-wide human factors initiatives.

## Hydraulics

### Findings

1. The downtime between Shuttle flights is much longer than commercial or military aircraft flights. This extended downtime allows component soft goods to dry out, increasing system maintenance.
2. The connection of the facility hydraulic lines to the Orbiter system is complicated by having to first install special brackets inside the aft of the Orbiter to support jumper lines that connect to the facility lines.
3. Systems can not be fully verified due to lack of test equipment or processes that adequately simulate actual flight conditions (see **Issue 5**).
4. The SIAT is concerned that compromised redundancies in the hydraulics system may exist, similar to those found in the Orbiter wiring.
5. Requirements documentation for hydraulics system testing and maintenance is incomplete, e.g., although hydraulic specification MIL-H-5440H was referenced in designing the Shuttle, no specific documentation was found to document the Shuttle's operational mode "waiver" from these requirements.
6. Orbiter maintenance practices have the potential to induce collateral damage to hydraulics systems.

### Recommendations

1. Shuttle actuator soft goods should be adequately wetted to prevent downtime seepage.
2. Consideration should be given to modifying the Shuttle internal hydraulic line routing to the mold line to permit efficient facility hydraulic hose connections.
3. The SIAT recommends comprehensive re-examination of maintenance and repair actions for adequate verification requirements (e.g., visual, proof test, or green run).
4. Where redundancy is used to mitigate risk, it should be fully and carefully implemented and verified. If it cannot be fully implemented due to design constraints, other methods of risk mitigation must be utilized.
5. All testing of units must be minimized and documented as part of their total useful life. Similarly, maintenance operations must be fully documented.
6. Maintenance practices should be reviewed to identify and correct those that may lead to collateral damage.
7. NASA and USA quality inspection and NASA engineers should review all CRIT 1 system repairs.
8. NASA should expand existing data exchange and teaming efforts with other governmental agencies especially concerning age effects.
9. A formal Aging and Surveillance Program should be instituted.
10. Standard repairs on CRIT1 components should be completely documented and entered in the Problem Resolution and Corrective Action system.
11. The criteria for and the tracking of standard repairs, fair wear and tear issues, and their respective FMEA/CIL's should be re-examined.

### Introduction

Maintenance requirements and operations were studied for the Space Shuttle, military and commercial aircraft for comparison. Federal Aviation Regulations (FARS) and the Eastern and Western Range Safety Requirements

---

(EWR 127-1) were assessed relative to the Shuttle maintenance requirements. Shuttle hydraulic system line routings were examined for redundancy purposes.

## **Assessment**

### **Kennedy Space Center Maintenance Items (standard)**

Major maintenance requirements for the Shuttle hydraulic system include: Water Spray Boiler leak checks and servicing (water and nitrogen) for flight; line and component inspections; flight control and actuator cycling; hydraulic fluid sampling; dissolved air removal and actuator filter delta pressure indicator inspections. The facility pumps, via fluid lines connected to the Orbiter, supply hydraulic fluid pressure required to cycle the actuators. The connection of the facility hydraulic lines to the Orbiter system is complicated by first having to install special brackets inside the aft of the Orbiter to support jumper lines that connect to the facility lines. Sampling of fluid for particulate count, purity and lengthy fluid de-aeration to 1% is also required.

### **Kennedy Space Center Failure-Induced Maintenance Items**

Seal leakage around actuators, insulation on hydraulic lines being crushed or soggy, seepage around hydraulic pump connections and component electrical problems represent the major failure-induced maintenance for the hydraulic system. Since the time between same Orbiter flights usually exceeds 4 months and sometimes 1 year or more, hydraulic system soft goods (seals) tend to "dry-out." Once activated, these seals tend to seep slightly until fully wetted. While this seepage is not considered a problem, and actuator failures are rare, the fluid sometimes finds its way under hydraulic line insulation causing its soggy appearance and subsequent maintenance, usually replacement. Electrical problems encountered are usually the result of adjacent component removals damaging heater or sensor wires.

### **Comparison to Federal Express Experience**

The level of hydraulic maintenance for Federal Express aircraft depends on the number of days since the last maintenance period. External visual inspections are performed on a flight by flight basis, with hydraulic fluid samples taken every year for purity and particulate count. De-aeration of the hydraulic fluid is not needed, since there is no requirement and at atmospheric conditions maximizes out at approximately 10 – 12 %. This lack of a requirement is apparently due to the design of the system, which allows for a "spongier" flight control system than the Shuttle. Since maintenance is performed reasonably soon after a flight, aerosurface frequency response tests are not required and only aerosurface extensions/retractions are performed. During one aerosurface inspection, a technician noticed a slower than normal rudder operation and subsequently checked and cleaned an upstream filter which was becoming contaminated. This data may lead to maintenance driven aerosurface response tests for Federal Express.

### **Comparison to DoD B-2 Experience**

The relatively new fleet of B-2 aircraft at Tinker Field will be undergoing its first depot level maintenance after five years of flying. Visual inspections using boroscopes are required in order to perform integrity checks of line runs inaccessible to standard inspections. Standard maintenance is performed after 50 hours of flight time and consists of running a Standard Built-In Test which checks out the flight control system. Post flight requirements consist of visual inspections of flight controls combined with Onboard Integrated Test System (OBITS) data, which checks the health of the hydraulic system and provides the ground crew a printout of system integrity. The B-2 has a fully instrumented hydraulic system, which detects system anomalies reducing ground turnaround operations. Delta pressure sensors located on actuator filters notify the onboard system of potential filter obstructions. De-aeration of hydraulic fluid is required down to 8%, which is a minimal operation when compared to the Shuttle's 1% requirement.

## Hydraulic Line Routing

Hydraulic system line routing for the Shuttle references military specification MIL-H-5440H, which is approved for use by all Departments and Agencies of the Department of Defense. Hydraulic system design (paragraph 3.2) states: "The hydraulic systems shall be configured such that failure of any two fluid systems resulting from combat or other damage which cause loss of fluid or pressure will not result in complete loss of flight control." Paragraph 3.8.3, which addresses system separation, states: "The systems necessary for safe flight shall be separated a minimum of 18 inches unless survivability and vulnerability analyses show that less separation is satisfactory." Hydraulic fluid line routing for the Orbiter from these requirements was investigated. No documentation or personnel recollections relieving the Shuttle from these requirements were obtained. Although lines are usually separated where space allows, in some instances, two lines of a three-line supported component will be run together, while routing the other leg alternatively. Strict adherence to MIL-H-5440H does not appear to have been carried out.

## Summary

Differences in the design, operation and life expectancy of the Shuttle hydraulic system drive maintenance requirements that are similar to other program requirements yet have unique elements. The maintenance performed on the Shuttle hydraulic system is more stringent, proactive, and frequent than in the B-2 and Federal Express programs. Still, concerns exist over incomplete documentation, potential compromised redundancy, and possible collateral damage to hydraulic systems for which the SIAT recommends the actions listed above.

## Hypergols and Auxiliary Power Unit

### Findings

1. Unlike Titan IV program, training is not given by the actual Shuttle flight hardware vendor, which removes technicians and engineers from a direct interface with the designers and creates reliance on manuals, drawings and maintenance procedures.
2. Thruster replacements caused by propellant valve leakage and propellant flight-half coupling replacements caused by couplings sticking open, represent the major failure-induced maintenance operations for Orbiter Maneuvering System/Reaction Control System.
3. A major maintenance item and source for leakage for the Auxiliary Power Unit system are the exhaust duct flange seals, which are installed during Auxiliary Power Unit installations.
4. Technicians sent to work in hazardous operations, while certified, are sometimes not familiar with the particular systems, thus exposing them and hardware to increased risk. Furthermore, safety or inspection processes during hypergol operations are not consistently implemented.
5. It is evident to the SIAT, based on information from problem disposition and KSC Shuttle Processing Human Factors Team event investigations, that an inadequate number of experienced, system specific technicians are available for critical operations.
6. USA Shuttle operations contractor appears to be moving toward a system specific technician approach, called the Advanced System Technician. This approach should provide the technicians with increased system level training required for hazardous system operations and should reduce risk.
7. The majority of the Shuttle hazardous operations involving fluid line connections are performed in Self-Contained Atmospheric Protective Ensemble (SCAPE), while other agencies' programs do not necessarily use full personnel protection. This is partly due to Shuttle system design, which does not provide for positive removal of hazardous fluids from the lines. Full personnel protection is also required since Kennedy Space Center guidelines require Self-Contained Atmospheric Protective Ensemble during operations that have a potential for no or very low potential for liquid flow (i.e., Kennedy Space Center is conservative).
8. Tank time and cycle data are not properly maintained between console manual logs and TACS system, which allows tank accumulated pressure hours to exceed design criteria in some cases (see **Issue 5**).
9. Fleet Leader testing does not properly represent actual operating environment, is not uniformly applied across sub-systems, and is not properly documented (see **Issue 5**).
10. There is also a concern about the electrical heating system used to maintain the hydrazine for the Auxiliary Power Unit and HPU at safe temperatures with adequate safety margins. While the heaters are fully redundant, the heater power lines tie back to a single point at the power source bus bar. A failure at this single point could result in some serious problems leading to early mission termination (not flight safety).

### Recommendations

1. Vendor supplied training should be evaluated for all critical flight hardware.
2. Due to obsolescence, Shuttle Reaction Control System propellant valves and propellant flight-half couplings should be replaced with ones that are more tolerant of the oxidizer environment.
3. Critical operations, especially those involving Self-Contained Atmospheric Protective Ensembles, must be staffed with technicians specifically experienced and properly trained with the operations.
4. Tank time and cycle data must be carefully logged to ensure safe life criteria are not exceeded.



5. Fleet Leader testing must be carefully scrutinized to ensure adequate simulation of operating conditions, applicability to multiple sub-systems, and complete documentation of results.
6. Serious consideration should be given to replacing the hydrazine power unit with a safer and easier to maintain advanced electric auxiliary power unit for the Thrust Vector Control hydraulic unit.
7. NASA and USA quality inspection and NASA engineers should review all CRIT 1 system repairs.
8. NASA should expand existing data exchange and teaming efforts with other governmental agencies especially concerning age effects.
9. A formal Aging and Surveillance Program should be instituted.
10. Standard repairs on CRIT1 components should be completely documented and entered in the Problem Resolution and Corrective Action system.
11. The criteria for and the tracking of standard repairs, fair wear and tear issues, and their respective FMEA/CIL's should be re-examined.
12. The SIAT recommends comprehensive re-examination of maintenance and repair actions for adequate verification requirements (e.g., visual, proof test, or green run).
13. Where redundancy is used to mitigate risk, it should be fully and carefully implemented and verified. If it cannot be fully implemented due to design constraints, other methods of risk mitigation must be utilized.

## Introduction

Maintenance requirements, hazardous operations and system training were studied for the Shuttle, Titan-4 and the NASA F-16 programs in support of the SIAT Hypergol / Auxiliary Power Unit assessment. Federal Aviation Regulations (FARS) and the Eastern and Western Range Safety Requirements (EWR 127-1) were assessed relative to the Shuttle maintenance requirements.

## Assessment

### Kennedy Space Center Maintenance Items (standard)

Orbiter Maneuvering System/Reaction Control System major maintenance requirements include: forward and aft helium system functionals; forward Reaction Control System and aft pod vapor level checks using electronic meters inserted behind removed skin panels; Orbital Maneuvering Engine (OME) ball-valve cavity propellant drain/purge requiring purge gas quick-disconnect (QD) hook-ups; and propellant/helium/nitrogen servicing for flight. Auxiliary Power Unit hazardous maintenance requirements are minimal outside of servicing 42 gallons of hydrazine per Auxiliary Power Unit for flight and performing toxic vapor checks of the Auxiliary Power Unit hardware.

### Kennedy Space Center Failure-Induced Maintenance Items

Thruster replacements due to propellant valve leakage and propellant flight-half coupling replacements caused by couplings sticking open represent the major failure-induced maintenance for Orbiter Maneuvering System/Reaction Control System. These failures can be attributed to the corrosive nature of the propellant oxidizer, nitrogen tetroxide and the way the system is used. The Shuttle, being a reusable spacecraft, does not have the luxury of starting each mission with new "clean" hardware. Replacement of a propellant component requiring system evacuation may affect others during the next mission. Forward thruster replacements drive removal of the Forward Reaction Control System, which requires transport of the Forward Reaction Control System to the Hypergolic Maintenance Facility (HMF) where repairs are performed. Aft thrusters can be replaced in the Orbiter Processing Facility (OPF). During Forward Reaction Control System or pod thruster removal operations, insulation blankets, Orbiter thermal tile or internal purge ducts may become damaged. This is due to the bulky Self-Contained Atmospheric Protective Ensemble (SCAPE) worn

by the technicians combined with the confined work area. A thruster (manifolds worth) is replaced on average about once every three flights per vehicle.

A major maintenance item for the Auxiliary Power Unit system is the exhaust duct flange seals, which are installed during Auxiliary Power Unit installations. Flange seals often leak following installation, requiring several sets of changeouts before the leak is within specification. Continued work around the exhaust duct can lead to damage of surrounding hardware such as exhaust duct temperature transducers. An estimate of fleet Auxiliary Power Unit change-out is once per year; leakage via the exhaust duct seals is encountered approximately once every two Auxiliary Power Unit replacements.

### ***Comparison to DoD and Titan***

F-16 fighter aircraft, which are flown for NASA at DFRF, rely on the activation of a hydrazine driven turbine called an Emergency Power Unit (EPU) in case of hydraulic or electric power failure in flight. Hazardous maintenance on the Emergency Power Unit is minimal, yearly and biyearly, since the 10 gallon hydrazine storage tank is mechanically isolated from the rest of the system, and activated only under emergency conditions. Hazardous maintenance required after hydrazine system activation includes reducing the ppm levels in the lines via a gas purge and replacing the storage tank with a newly fueled one. Connections between the storage tank and the line run to the catalytic bed are of the quick-disconnect type. Prior to removing the aircraft skin panel to perform this infrequent operation, a system integrity vapor check is performed by visually inspecting a hydrazine sensor through an inspection window.

EWR 127-1<sup>5</sup> affects the Titan 4-B program by providing a common set of requirements to minimize safety risks and maximize user objectives. For an expendable program such as Titan 4-B, recurring maintenance on hypergol-contaminated systems is not an issue, since there are no long-term detrimental propellant effects. The Titan 4 vehicle has pre-valves, which isolate the propellant tanks from the rest of the engine. Once the pre-valves are opened, flooding the engine manifold with propellant at 16 seconds prior to launch, a 48-hour life limit is invoked on the downstream system. This limit ensures soft goods (seal) integrity, and if violated the entire system is changed out.

### **Self-Contained Atmospheric Protective Ensemble Operations**

Kennedy Space Center technicians working in operations requiring Self-Contained Atmospheric Protective Ensemble have a variety of certifications and on the job training requirements beyond the general Self-Contained Atmospheric Protective Ensemble suit use. These include general system level courses and specific operation certifications. As the technicians become more experienced, they will have higher levels of training certificates and on the job training packages allowing them to work on more complex hardware operations. The new Self-Contained Atmospheric Protective Ensemble technician initially enters an operation as an observer, then as he/she gains experience becomes the buddy of a more experienced technician. Personnel involved with hazardous operations are required to participate in engineering pre-test briefings and area walkdowns. The shop supervisor ultimately assigns the most qualified individual for hazardous operations based on the complexity of the job and the availability of personnel. Technicians entering the work site are regarded by engineering as having been informed of the operation, either by the technicians' superiors or having taken part in the walkdown, and are already familiar with the hardware and task at hand. Violation of this prior experience condition has resulted in dangerous spills of hydrazine on an Orbiter in the past (OPF-3 Fuel Leak, OV102, August 22, 1999).

F-16 technicians who work on the hydrazine system receive training from an Air Force technical school where a general overview of the system is given. Prior to performing any hazardous operation, personnel pre-test briefings and operational dry runs are performed. Breathing air (Scott air-packs) is rarely used except during on occasion where the hydrazine vapor level exceeds 0 ppm such as during hydrazine storage tank replacement after activation.

Technicians working in Self-Contained Atmospheric Protective Ensemble on the Titan 4-B program are certified experts on their particular system. Prior to working on hazardous systems, technicians are required to have completed their on the job training package which includes specific system courses, such as the 5-day

hands-on Aerojet engine class, given by the major element contractor. These courses give technicians and engineers a direct interface with the manufacturers / designers as opposed to relying only on manuals, drawings and maintenance procedures for education.

## **Advanced System Technician**

The concept of Shuttle "system specific" technicians or "one tech fits all" has been discussed several times in the past and depending on the level of involvement or concern, whether from the technical side (engineering and technician) or the management/personnel side, there are advantages and disadvantages (see Finding 6).

### Advantage

Technicians who are highly trained and work on one particular system have the advantage to follow an operation from day to day, allowing for safer operations. The "system specific technician" concept leads to a higher quality product as a feeling of system pride resides with the technician and his/her group. This leads to less hardware damage, minimizing close calls and a general decrease in personnel and property risk. These "system specific" technicians would be fully experienced with the hardware, having gone through a rigorous degree of system level training and awareness. Hazardous Self-Contained Atmospheric Protective Ensemble and emergency situations would be handled with a higher degree of system knowledge and therefore safety, since system design features and potential problem areas would be fully understood. During Self-Contained Atmospheric Protective Ensemble operations involving hypergols this understanding is extremely important, as a small amount of leaking liquid or heavy fuel vapor could start a fire. An adequate number of system specific technicians would eliminate the need for using technicians with less than average system level experience.

### Disadvantage

The major disadvantage of the system specific technician concept is the inefficiency of manpower utilization. Under this system, technicians would not be utilized in the best manner, since there would be significant technician downtime until their system work was scheduled. Specific system operations between different Orbiters could initially be staggered to take advantage of the system specific concept. Yet, unforeseen hardware failures and scheduling conflicts would eventually require multiple specific system operations (on different Orbiters) to occur at the same time, requiring more personnel.

The contractor, United Space Alliance (USA), has recently announced a restructuring program for engineering and the shops. The "Advanced System Technician" concept will provide "in depth" system specific training equivalent to an entry or low level engineer. These individuals will be tasked with performing some of the functions of the inspector, engineer and technician and will follow a specific Orbiter through its turnaround maintenance (see **Issue 4**).

## **Summary**

Differences in the design, operation, and life expectancy of the Shuttle hypergolic / hydrazine systems drives maintenance requirements that are similar to other programs requirements yet are unique. The maintenance performed on the Shuttle Orbiter Maneuvering System/Reaction Control System and Auxiliary Power Unit systems is more stringent, proactive, and frequent than in the Titan-4B and F-16 programs. Furthermore, Shuttle hypergolic system leak check requirements are more stringent than those on flight vehicles covered by the Eastern and Western Ranges (including Titan 4-B). While stringent maintenance requirements and system checks are in place for the Shuttle, the findings and recommendations listed above still require attention and correction.

## **Problem Reporting & Tracking Process**

### **Findings**

1. The Problem Resolution and Corrective Action reporting system appears designed from the perspective of data to be kept ("bottom up"), not from the perspective of decisions to be made ("top down"). It does not provide high confidence that all potentially significant problems or trends are captured, processed, and visible to decision-makers.
2. Effective utilization of the Problem Reporting and Tracking system requires specific expertise and experience to navigate and query reporting systems and databases.
3. Missing and inconsistent events, information, and criticality lead to a false sense of security.
4. Tracking and trending tools generally lack sophistication and automation, and inhibits decision support. Extensive "hands-on" examination and analysis is needed to process data into meaningful information.
5. Critical information may be lost and ignored, and problems may be repeated due to weaknesses in reporting requirements, and processing and reporting procedures.
6. The fragmented structure of the Problem Resolution and Corrective Action system, built from legacy systems, minimizes its utility as a decision tool.

### **Recommendations**

1. The SSP should revise the Problem Resolution and Corrective Action database to include integrated analysis capability and improved problem classification and coding. Also, improve system automation in data entry, trending, flagging of problem recurrence, and identifying similar problems across systems and sub-systems.
2. The root cause(s) for the decline in the number of problems being reported to the Problem Resolution and Corrective Action system should be determined, and corrective action should be taken if the decline is not legitimate.
3. The root cause(s) for the missing problem reports from the Problem Resolution and Corrective Action system concerning Main Injector liquid oxygen Pin ejection, and for inconsistencies of the data contained within the existing problem reports should be determined. Appropriate corrective action necessary to prevent recurrence should be taken.
4. A rigorous statistical analysis of the reliability of the problem reporting and tracking system should be performed.
5. Standard repairs on CRIT1 components should be completely documented and entered in the Problem Resolution and Corrective Action system.
6. Reporting requirements and processing and reporting procedures should be reviewed for ambiguities, conflicts, and omissions, and the audit or review of system implementation should be increased.
7. The Problem Resolution and Corrective Action system should be revised using state-of-the-art database design and information management techniques.
8. All critical data bases (e.g., waivers) need to be modernized, updated and made more user friendly.

### **Introduction**

Problem tracking and trending is considered by the SIAT to be a crucial process for the safe performance of the Shuttle, given the Space Transportation System's complexity and age. Risk assessment and management

cannot be successfully accomplished, it is believed, without full disclosure of current, complete, and relevant information generated by problem tracking, resolution and trending. This view is supported by studies<sup>6</sup> that find the majority of failures in complex engineering systems are caused by organizational or process errors. Process errors related to problem tracking and trending include<sup>7</sup> the following:

- overlooking and/or ignoring defects
- missing signals or valuable data due to inadequate inspection or maintenance policy
- tardiness in correcting defects
- breakdown in communication

Accordingly, a group of technical contributors was formed to assess the Shuttle system for problem identification, resolution, recurrence control, and traceability. The Shuttle system consists of numerous data bases, including transactional Problem Resolution And Corrective Action (PRACA), waiver, hazard, time/age/cycle databases among others (see Table 3). These databases are used to report problems, track corrective action, and collect data for trend analysis. The specific objectives of the assessment were to:

- examine the quality of the databases and data management techniques (i.e., determine if the database design supports modern requirements);
- examine the quality of the data in the system (i.e., determine if the right data are getting into the system); and
- examine the quality of the information in the system (i.e., determine if the data contained in the system is useful for decision-making).

To make the assessment, technical contributors were briefed by Space Shuttle Program (SSP) personnel on the database organization, structure, and management, and on problem reporting requirements and procedures. Documents were reviewed, including a Marshall Space Flight Center Independent Assessment of Problem Resolution and Corrective Action [draft, 8/99], a International Astronautical Federation (IAF) paper concerning Marshall Space Flight Center trending techniques [1997], a wiring trending study performed by Kennedy Space Center [10/99], the Problem Resolution and Corrective Action System Requirements and Procedures Documents<sup>8</sup> [1996/97], a Reliability-Centered Maintenance (RCM) Report generated by Kennedy Space Center [1/99], and the Aerospace Safety Advisory Panel Annual Reports. Several "hands-on" sessions, were held, which included interacting with and querying of the databases to search and obtain data and information from the system. These sessions were attended by two SSP "experts" to aid in formulating the queries and navigating the system. As a quantitative test of the system, a specific problem, namely that of the Main Injector liquid oxygen pin ejection, was traced and the results compared to those briefed to the SIAT by Boeing-Rocketdyne.

## **Assessment**

### **Quality of Database and Data Management**

The problem reporting databases have a distributed architecture, with problems reported and entered from a variety a geographically diverse sites. The three NASA centers, Johnson Space Center, Kennedy Space Center, and Marshall Space Flight Center, each have their own Problem Resolution and Corrective Action database: at Kennedy Space Center, the problem reports are mostly associated with non-conformances and in-family problems; at Johnson Space Center, design and out-of-family problems related to Orbiter are tracked; and at Marshall Space Flight Center, problems associated with Space Shuttle Main Engine, Solid Rocket Booster, External Tank, and Reusable Solid Rocket Motor are reported. In addition to these transactional databases at Johnson Space Center, Kennedy Space Center, and Marshall Space Flight Center, contractors may also have internal databases in which problem reports are initiated. Some of these contractor databases cannot communicate electronically with the NASA Problem Resolution and Corrective Action systems so problems have to be phoned or faxed in. The "core data" from the transactional databases are currently uploaded daily to a web-based, data warehouse called ADAM.

In addition to Problem Report databases, there also exist numerous other electronic databases that contain and maintain data needed for problem trending and risk assessment. These are shown in Table 3. These databases are maintained at the data warehouse level as authoritative sources. However, data from the authoritative electronic source are often downloaded to transactional databases for ease of accessibility and manipulation. The authoritative source for the FMEA/CIL is a paper document.

Database	Configuration Management
Waiver	electronic authoritative source
Time/Age/Cycle	electronic authoritative source
Launch Commit Criteria	electronic authoritative source
DRTS flight software	electronic authoritative source
Hazards	electronic authoritative source
In-Flight Anomaly	electronic authoritative source
FMEA/CIL	paper authoritative source

Table 3 -- Databases for Process/Problem Reporting

The number of databases and the mixture of paper and electronic information sources makes configuration management difficult. For instance, changes to the FMEA/CIL are made at the transactional database level, but must go to the Program Review Change Board for review and approval. The approved changes are distributed back to the sites via a paper revision to the authoritative source. The databases must then be updated to reflect the approved revision. This type of process leads the information at the working level to be out-of-sync with Program level approved information. Periodic corrections must be made to realign the local databases with the Program level databases.

The documentation for the databases requirements and procedures were found to be up-to-date and available. However, training manuals and search tips were unavailable, neither on-line nor in a paper source.

The Problem Resolution and Corrective Action system is currently transitioning from a mainframe application (Program Compliance Assurance and System Status) to a data warehouse (ADAM) with uniform web-based interfaces. On-line searches were extremely time-consuming, either because of slow search engine capabilities or data transmission speed.

Experienced personnel could navigate the system and formulate queries easily; however, training and experience are required for effective system use. Even with expert assistance, however, queries were inefficient due to simplistic search capabilities. Pruning of large numbers of search results was impossible because searches could not be formulated to exclude certain data strings or fields. Furthermore, trending capabilities lack sophistication and automation (an attempt to improve trending capabilities is the use of Laplace methods by Johnson Space Center Safety, Reliability & Quality Assurance<sup>9</sup>). Reports generated directly from the Problem Resolution and Corrective Action system are mostly tabulated data fields that must then be dumped to a program like EXCEL for further processing. All but the most rudimentary trends (occurrences over time) require significant post-processing to produce (see **Quality of Information** sub-section below).

### Quality of Data

As a first measure of the quality of data in the problem tracking system, the number of problem reports being entered into the system was examined. Using the Kennedy Space Center RCM report of January, 1999, the number of Problem Reports entered into the Kennedy Space Center Problem Resolution and Corrective Action system was plotted as a function of time (Orbiter flow). Although there is some scatter in Problem

Report count, it is clear from the data shown in *Figure 4 -- Problem Reports by Orbiter* that there is a decline in the average number of Problem Reports after 1995. This decline may reflect changes in reporting requirements, such as the increase in allowable discrepancies due to Fair, Wear and Tear, and improvements in process or hardware. However, the decline may also reflect the reduction in Government Mandatory Inspection Reports, quality assurance personnel ("second set of eyes"), and/or other checks and balances on the system. This finding is corroborated by the audit (draft) of the Marshall Space Flight Center Problem Resolution and Corrective Action system by Safety & Mission Assurance personnel: "Recent numbers of problems being reported by the contractors into the Marshall Space Flight Center Problem Resolution and Corrective Action system ... are down...." The report went on to state the concern that "these reductions do not seem to be completely justified by test schedules, revision from in-family screening and similar requirements adjustments, or improved hardware." The decline in Problem Report reports requires deeper investigation to ascertain its true cause and acceptability.

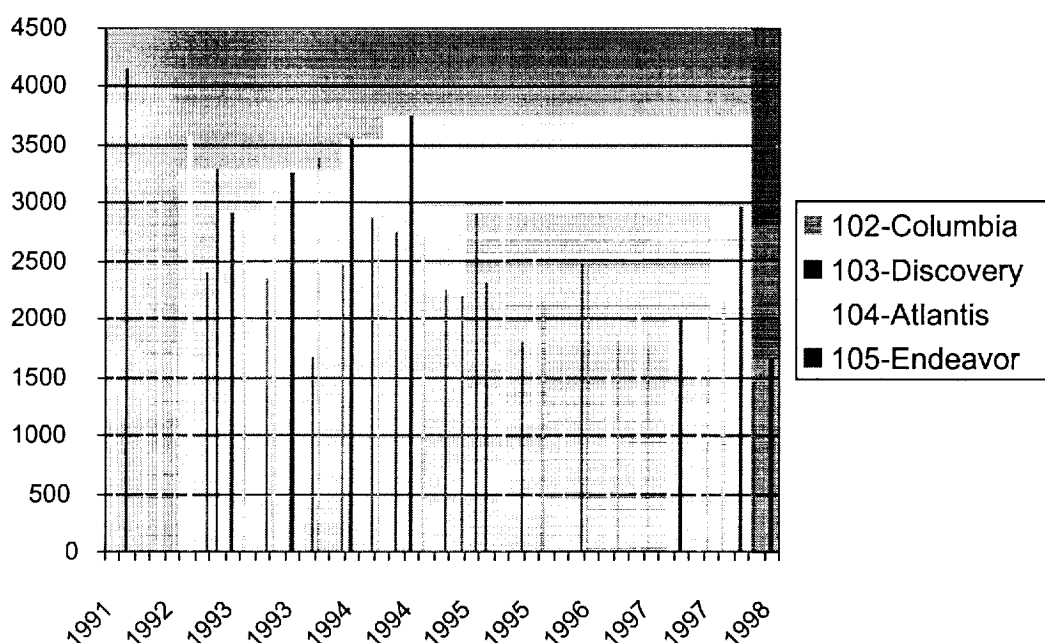


Figure 4 -- Problem Reports by Orbiter

A second quantitative assessment of the data in the Problem Resolution and Corrective Action system was made by tracking a known problem, namely that of the Main Injector liquid oxygen pin ejection. Both the Marshall Space Flight Center Problem Resolution and Corrective Action system and the data warehouse ADAM were searched for Problem Reports addressing pins in the Space Shuttle Main Engine. Only three of the ten known occurrences of Main Injector liquid oxygen pin ejection were recorded in either system. As shown in *Figure 5 -- Problem Tracking Example: SSME Liquid Oxygen Post Pins*, which is the Rocketdyne-Boeing analysis of the pin ejection history, only occurrences on engines 2308 in 1984, 2022 in 1990, and 2107 in 1994 were reported in the Problem Resolution and Corrective Action system. In contrast, the historical record provided by Rocketdyne-Boeing for problem close-out on the Problem Report for the 1994 occurrence listed a different set of three occurrences: two that occurred before 1980 and the occurrence on engine 2022 in 1990. Further examination of the Problem Report records for Main Injector liquid oxygen pin ejection indicated that the CRIT levels assigned to the functionality and the hardware associated with pin ejection varied from 3/\_, 3/1, to 1/1. Also varying in degree and fidelity was the resolution description provided on each Problem Report.

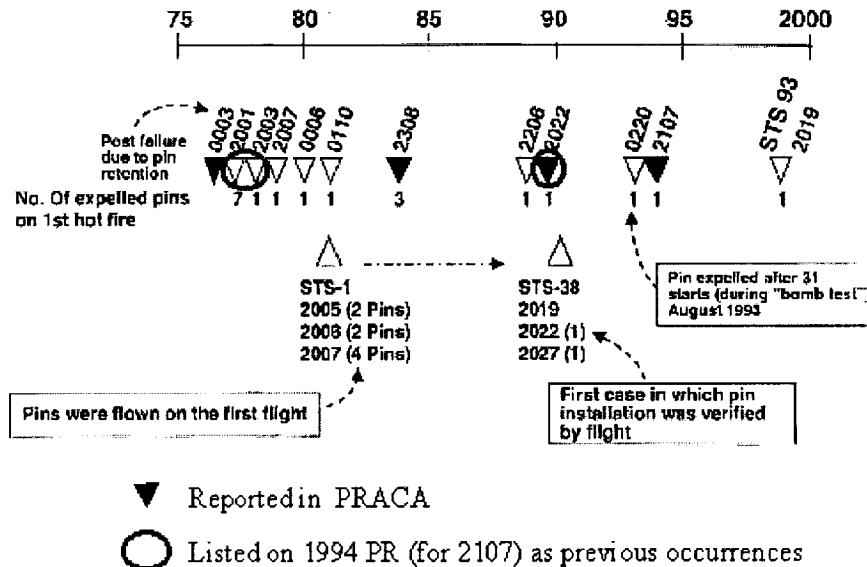


Figure 5 -- Problem Tracking Example: SSME Liquid Oxygen Post Pins

It is clear from the results of this test of the Problem Resolution and Corrective Action system that the data concerning the occurrence of pin ejection was both incomplete and inconsistent. Confusion concerning the reportability of the problem of pin ejection was still evident during discussions held with engineers as part of this assessment. Pinning of the liquid oxygen post was clearly considered a standard repair and pin ejection understood to be a benign condition. So although the criticality of the hardware (CRIT 1) and the timing of the ejection (during first hot-fire after pinning) require the occurrence to be reported in the Problem Resolution and Corrective Action system, problem reports concerning pin ejection were not always made. Had they consistently been reported, the 1 in 10 probability of occurrence may have raised concern over flying a pinned post on STS-93 without prior hot-firing.

In the course of tracking the liquid oxygen pin ejection history, several other concerns arose for the quality of the problem reporting and tracking system. The searches in the Problem Resolution and Corrective Action system databases for problems related to pins in the Space Shuttle Main Engine netted a number of reports concerning a similar problem of pin ejection from liquid oxygen posts in the fuel and oxidizer pre-burners. No cross reference was found between the two types of pin ejection in the Problem Resolution and Corrective Action system; the problems had many similarities, including the use of friction fit to retain the pins and the criticality of the hardware. Further, it was noted on a 1994 Problem Report for missing liquid oxygen support pins on the oxidizer pre-burner that pin ejection was not a failure mode considered in the FMEA/CIL for the oxidizer pre-burner (although it was for the fuel pre-burner). Had there existed some sort of cross reference, the lack of a Failure Modes and Effects Analysis for pin ejection on the Main Injector liquid oxygen post pin may have been caught and may have prevented the flight of a previously untested pinned post on STS-93.

Another concern arose over trying to determine whether a waiver or deviation was required to be approved for flight of a pinned liquid oxygen post without prior hot-fire testing. A search of the waiver database for the string "hot-fire" proved unsuccessful and more refined searches were not supported by the current search engine. Hence, the waivers listed for flights in which engines were flown with pinned posts and without prior hot-firing (STS-38, 40, 42, 52, 56, 75, and 93). The list for STS-93 alone contained 350 pages of waivers and deviations dating back to 1988, although none for Space Shuttle Main Engine pinning or hot-firing were noted. These results raised concerns over the number and age of the waivers approved for each flight and the difficulty in tracking these waivers in the database system (see also **Risk Assessment & Management**).



## Quality of Information

The problem reporting system was examined to determine how readily and how well the data contained in the system could be processed to provide information for decision making. Requirements and capabilities for problem trending were found to differ for each element of the Shuttle. For the Orbiter, the Prevention/Resolution Teams decide if or when Problem Resolution and Corrective Action system data analysis is needed and what type is performed. For propulsion elements, contractors perform trending as needed for problem resolution. Marshall Space Flight Center Safety & Mission Assurance periodically examines problem trends on CRIT 1/1R hardware in the Space Shuttle Main Engine only.

In all cases, trending is rudimentary; very little numerical or statistical analysis is performed. Furthermore, no automated flags exist within the problem reporting system to alert engineers or Safety & Mission Assurance personnel to high incidences of problem recurrence.

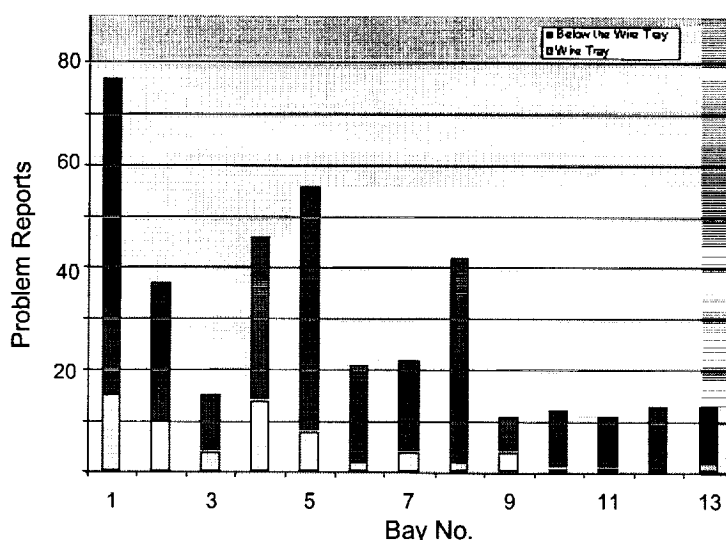


Figure 6 -- Kennedy Space Center Wiring Trending

In addition to assessing general trending capabilities, two trending studies made with data in the Kennedy Space Center and Marshall Space Flight Center Problem Resolution and Corrective Action systems were examined in detail. The first such study concerned wire damage problems. In order to assess the root cause of wire damage, trends were needed that distinguished the type of wire damage (i.e., insulation damage, exposed conductors, conductor damage) as a function of location of occurrence in the Shuttle. An example trend report is shown in *Figure 6 -- Kennedy Space Center Wiring Trending*. To provide this information, a team of 10 engineers and 3 quality inspectors worked for 1 week reviewing Problem Reports in the Kennedy Space Center Problem Resolution and Corrective Action system. This intense effort was needed because the data contained in the system lacked standardization and fidelity and needed to be assessed and interpreted by the engineers in order to be meaningful. In some cases, the data did not exist or could not be resurrected.

An extensive review of records was also required to provide trend information for the Space Shuttle Main Engine using the Marshall Space Flight Center Problem Resolution and Corrective Action system. In a 1997 paper on Space Shuttle Main Engine trending for an International Astronautical Federation Symposium, the methodology used to trend Space Shuttle Main Engine problems was described. First the problems were screened to obtain only CRIT 1/1 problem reports for a certain piece of hardware. After this initial screening, the records had to be reviewed to: "assure the accuracy of the coding," obtain "a preliminary understanding of the issues involved," and assure the "completeness of the data" before any trending could be performed.

Both of these studies indicate that the data contained in the problem reporting system cannot be processed quickly or directly by the system to obtain information for decision-making. Extensive examination and interpretation is needed to process the data for trending, making the system inefficient if not ineffective.

## **Potential Systemic Issues**

The concerns identified in specific tests of the problem reporting system suggest that systemic issues may exist. Several potential sources of systemic problems were found, namely weaknesses in reporting requirements, processing procedures, and reporting procedures.

### **Reporting Requirements**

Several weaknesses were identified in the problem reporting requirements for the Shuttle per National Space Transportation System documents (NSTS 37325 and NSTS 08126). In some cases, the requirements appear to be unclear or conflicting; confusion exists, for instance in the Main Injector pin ejection problem, over whether a standard type repair issue should be reported for CRIT 1 hardware. Other requirements allow interpretation of the directive, such as those requiring identification of "significant" problems or processes that are "out-of-control." Finally, the reporting requirements appear incomplete: for instance, only Government Industry Data Exchange Program alerts are required to be entered but not other potentially relevant information such as Federal Aviation Regulations or DOD lessons learned (e.g., Titan wiring failure).

These findings are corroborated by the Marshall Space Flight Center draft audit report. This audit found that reporting processes must only meet the intent of requirements, leaving "compliance open to interpretation both by NASA and the contractor." The audit also noted several specific differences between contractor implementations and National Space Transportation System requirements in areas "regarding rigor of analysis, processing flow, closure rationale development, and reportability evaluation." The report concludes that while the reporting process "seemed to be working," this is more the result of "personal intervention and common practice" rather than documented obligations.

Based on these observations, the potential exists for problems to go unreported and uncorrected due to ambiguities in reporting requirements.

### **Processing Procedures**

Problem processing procedures were also examined for potential weaknesses. It was found that several decision points (see *Figure 7 -- Problem Processing & Dispositioning*) exist in the procedures in which a problem and important attendant information can fail to enter the Problem Resolution and Corrective Action system. First, a problem has to be judged reportable, a judgment subject to the problems of uncertainty, interpretation, and lack of information described above. Decisions concerning problem reportability may occur at the technician level, with little engineering and/or Safety & Mission Assurance oversight or review.

Once reported, the problem is then screened to be either in-family or out-of-family to determine whether problem resolution is a Shuttle Flight Operations Contract or NASA responsibility. The distinction between in- or out-of-family has been scrutinized by the Aerospace Safety Advisory Panel: the panel's 1995 finding identified concern over adequate "development and implementation of the definition of an out-of-family situation." The distinction between in-family and out-of-family also concerns some of the personnel reporting problems, for instance, those at Palmdale, who claim they have never liked or really understood definition. And while formal review is given to designated out-of-family problems, review of those designated as in-family problems (posted to a website) is voluntary.

Finally, Orbiter problem tracking and resolution is ultimately the responsibility of the Prevention/Resolution Teams. Prevention/Resolution Teams possess significant autonomy and discretion in addressing Problem Reports. For instance, team membership is decided by the team leader and may vary with the problem. These teams do not typically include inspectors or quality assurance personnel. The team may develop "unique criteria for problem reporting and processing where required." Team activity is recorded using

meeting minutes; minutes are not entered into the Problem Resolution and Corrective Action system, although some Prevention/Resolution Teams post minutes on websites.

These observations cause concern that processing procedures do not provide sufficient visibility of problem occurrence and resolution and may allow problems to be lost from the system.

#### PROBLEM PROCESSING AND DISPOSITIONING

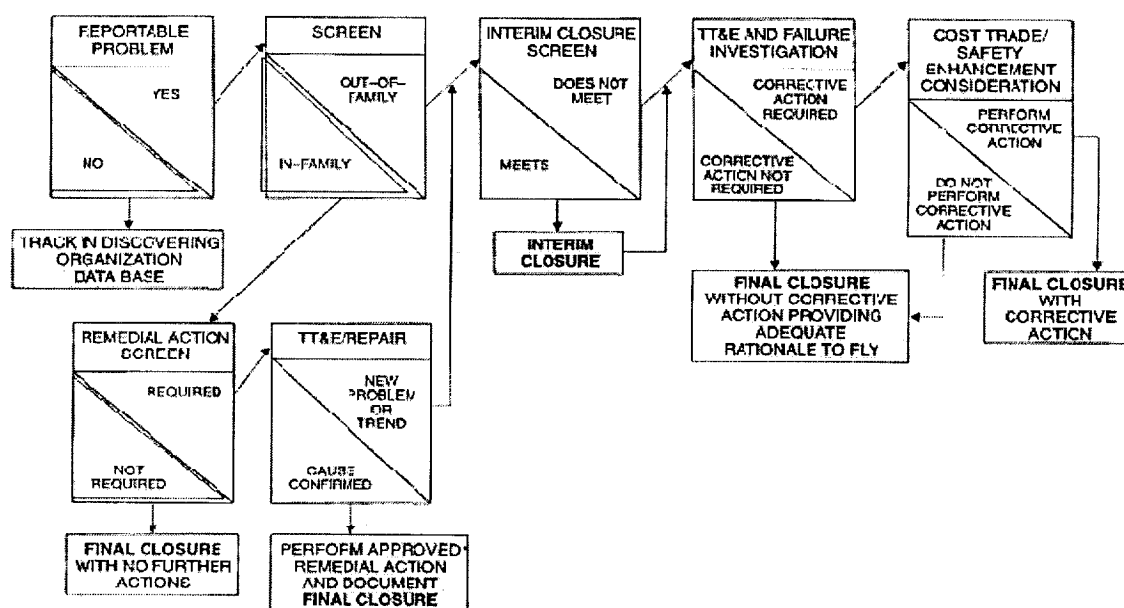


Figure 7 -- Problem Processing & Dispositioning

#### Reporting Procedures

Several concerns were also identified in reporting procedures. It was found that the procedures may not ensure data standardization or fidelity. The system lacks the automation needed to check data entry for completeness and accuracy. As apparent in *Figure 8 -- Potential Weaknesses in Reporting Procedures - A*, there is little validation provided for data elements entered into the Problem Resolution and Corrective Action system, even for crucial pieces of data such as the CRIT level. This lack of automation is also apparent in written procedures for hardware identification, as shown in *Figure 9 -- Potential Weaknesses in Reporting Procedures - B*. Note the warning provided that if the data are not entered, then future failure searches will fail to identify the problem.

These types of procedures place undue reliance on the human interfaces to the system and makes tracking and trending ineffectual due to missing or incorrect data. Finally, the mixture of formats in which problems are reported, including paper, electronic, fax, and phone, may lead to obsolete or lost data as well.

SSP PRACA DATA ELEMENTS - Continued

NO.	ELEMENT NAME	TYPE	USAGE	IN	OUT	CCC	BY	EDIT	DEFINITION
25C4	MANUFACTURER		JKM	6 AN	60 AN			TABLE	Manufacturer of NCA. Reference CAGE codes.
25D	EIM		JKM				DC		End Item Model (EIM).
25D1	NOMENCLATURE		JM	30 AN	30 AN			NONE	Name of EIM.
25D2	PART NO		JKM	25 AN	25 AN			NONE	Part number of EIM.
25D2A	MFR PART NO.		JK	25 AN	25 AN		CR	NONE	Manufacturer part number, if different.
25D3	SERIAL/OTNO		JM	15 AN	15 AN			NONE	Serial/lot number EIM.
25D4	MANUFACTURER		JM	5 AN	60 AN			TABLE	Manufacturer of EIM. Reference CAGE codes.
26A	RMFA NO	RC2	JM	20 AN	20 AN	1	CR	NONE	The Failure Modes and Effects Analysis (FMEA) number which addresses the failure mode of failed element/ LRU/SRL (to lowest level possible).
26B	FAILURE MODE	RC1	JKM	3 AN	12 AN	1	CR	TABLE	A description of the manner in which an item failed. Reference: JSC - Orbiter and GFE PRACA Requirements (JSC-24636) KSC - PRACA User's Guide (LSO-090-171-1143) MSFC - PRACA User's Guide (MFGASS-UG-0003)
26C	CIL RATIONALE	RC2	JKM	1 A	1 A		DC	Y OR N	Is CIL waiver revision required? (Y or N)
27	CRITICALITY								
27A	FUNCTIONAL CRITICALITY	RC1	JKM	2 AN	2 AN	1	CR	TABLE	See glossary NSTS 08126.
27B	HARDWARE CRITICALITY	RC1	J	1 AN	1 AN	1	CR	TABLE	See glossary NSTS 08126.
27C	LRU CRITICALITY	RC1	JKM	2 AN	2 AN	1	DC	TABLE	The worst-case criticality of the LRU or component based on NSTC FMEA/CIL failure modes.

No validation

Validated against a code table, if not blank

Figure 8 -- Potential Weaknesses in Reporting Procedures - A

BLK NO.	EXPLANATION
36 thru 47 (see below)	<p><b><u>FAILURE HARDWARE LEVELS OF IDENTIFICATION</u></b></p> <p><b>GENERAL:</b> WHEN PREPARING THIS SECTION OF THE Q-3, BE MINDFUL OF THE NEED TO UTILIZE THE DATA FOR FAILURE HISTORY SEARCHES. THERE ARE FIELDS FOR THE SRU, SUB-SRU, SUB MODULE, PART, OTHER, ETC.</p> <p><b>PLEASE USE BLOCK 36 FOR THE LRU, AND BY ALL MEANS ENTER THE SRU OR LOWER LEVELS ON THE FORM. IF 2 LRUS ARE IMPLICATED IN AN UNEXPLAINED ANOMALY, PUT ONE IN BLOCK 36 AND THE OTHER IN BLOCK 42B. IF YOU FAIL TO ENTER THIS DATA, IT WILL NEVER COME UP DURING FUTURE FAILURE SEARCHES.</b></p>

Figure 9 -- Potential Weaknesses in Reporting Procedures - B

## **Summary**

It is clear to the SIAT from this assessment that the problem tracking and reporting system requires significant improvements and enhancements. The recommended changes address not only the database and search and trend tools, but also concern the reporting and tracking requirements and procedures themselves. Complete, consistent, and relevant information must be directly accessible and quickly available for risk management and decision making. It is the belief of the SIAT that such information is neither entered, entered correctly, nor readily retrieved in the existing system. The findings and recommendations given above must be fully addressed.

## Propulsion

### SSME, External Tank, Solid Rocket Booster, Reaction Control System

#### Findings

##### Space Shuttle Main Engine

1. The SIAT commends Rocketdyne for their in-factory Foreign Object Debris (FOD) prevention efforts. However, the treatment of internal Foreign Object Debris generated during engine operation or from routine in-process maintenance between flights, requires an extensive review. The pin ejection incident on STS-93 is a prime example of deficiencies in the system.
2. The SIAT considers that a serious lapse in judgment and/or in attention to the engine data base occurred, which allowed two pins to be used in STS-93, without ground test verification firing.
3. The SIAT believes that the handling of the pin insertion and test as a standard repair significantly contributed to the subsequent pin ejection and the nozzle damage during STS-93 flight. Its treatment as a standard repair precluded management visibility of the frequency of LOX post deactivation and the evidence that hot-fire verification was integral to the repair process. Standard repairs may be acceptable in some cases; however, repairs of CRIT 1 hardware require greater scrutiny. Of the 450-500 potential causes of CRIT1 failures in the Space Shuttle Main Engine, more than 200 can be treated by standard repairs.
4. The SIAT finds that there was pervasive evidence that liquid oxygen post pin insertion required hot-fire verification. Of 19 pins ejected during ground testing, all but one were ejected during the first engine firing.
5. There are three major hot gas mechanical joints inside the Space Shuttle Main Engine that represent potential leakage paths, and should be appropriately reviewed. These are: the power head hot gas ducts, the Main Combustion Chamber to power head joint, and the Main Combustion Chamber to nozzle joint.
6. In addition to the cryogenic mechanical joints between the External Tank and the Space Shuttle Main Engine inlets, there are a number of other cryogenic fluid mechanical joints that represent potential risks.

##### Solid Rocket Booster

1. Repeatability and quality of the grains in the Solid Rocket Booster motor segments may not be as thorough as it was in the earlier phases of the program. The SIAT is concerned that the quality control for these elements after the motor has been poured is a major potential risk area.
2. The whole lower case joint for the Solid Rocket Booster submerged nozzle, including the hot gas seals, thermal barriers and flex joint/seal appear to be located in a very high thermal and mechanical stress zone. The concern for this design is exacerbated because the nozzle and associated joints are reused many times.
3. The Thrust Vector Control (TVC) power unit for the Solid Rocket Booster uses a hydrazine fueled gas generator to drive a turbine, which in turn drives the nozzle swivel joint hydraulic pump to achieve the desired Thrust Vector Control range. The use of a hydrazine system as the power source for this highly stressful environment and reusable application (including parachuting into the ocean and subsequent recovery) is viewed as a high-risk situation for many reasons. The same concerns apply to the hydrazine

---

powered hydraulic Auxiliary Power Unit used on the Orbiter for various emergency and normal final landing hydraulic actuator functions (flaps, ailerons, elevons, etc).

## Reaction Control System

1. Both the Orbiter Maneuvering System and Reaction Control System hypergolic (i.e., earth storable) propulsion sub-systems on board the Orbiter represent, in the opinion of the SIAT, risk areas in several ways (e.g., age of hypergolic propulsion systems will require increased maintenance, difficult access and working conditions due to Self-Contained Atmospheric Protective Ensemble suits, extreme reduction in experienced crews with minimal OEM involvement).
2. Orbiter Maneuvering System and Reaction Control System pod feed systems were originally integrated by the old Rockwell Corporation from now defunct suppliers. Most of the day-to-day operations and maintenance work is being done by less experienced people at USA. Against this background, it was reported to the SIAT that it is planned to modify the system to add cross feed lines between the forward and aft Orbiter Maneuvering System and Reaction Control System pods, through the mid-body or one of the wings, with additional plumbing and quick disconnects for refueling of Space Station (ISS) propulsion modules. All of this adds to the risk concerns already expressed by the SIAT for this propulsion element.

## Recommendations

1. All internal Foreign Object Debris (e.g., pins) occurrences during the program should be listed, with pertinent data on date of occurrence, material, and mass. The internal Foreign Object Debris FMEA/CIL's and history should be reviewed and the hazard categorized based on the worst possible consequence.
2. Standard repairs on CRIT1 components should be completely documented and entered in the Problem Resolution and Corrective Action system.
3. Any type of engine repair that involves hardware modification -- no matter how minor (such as liquid oxygen post pin deactivation) -- should be briefed as a technical issue to the program management team at each Flight Readiness Review. The criticality of a standard repair should not be less than basic design criticality, based on worst case consequences, and all failures of standard repairs should be documented and brought to the attention of the Material Review Board.
4. The SIAT recommends comprehensive re-examination of maintenance and repair actions for adequate verification requirements (e.g., visual, proof test, or green run).
5. There are a number of cryogenic fluid mechanical joints and hot-gas mechanical joints that represent potential risks that should therefore be examined in detail.
6. NASA and USA quality inspection and NASA engineers should review all CRIT 1 system repairs.
7. The criteria for and the tracking of standard repairs, fair wear and tear issues, and their respective FMEA/CIL's should be re-examined.
8. The true mission impact of a second main engine pin failure (internal engine foreign object debris) during flight, similar to that which took place last July, should be determined.
9. The SSP should consider more frequent lot sample hot fire testing of Solid Rocket Booster motor segments at full-scale size to improve reliability and safety and verify continued grain quality.
10. The design of the Solid Rocket Booster, and the post-recovery inspection and re-certification for flight should be looked at and analyzed in careful detail by follow-on independent reviews.
11. Where redundancy is used to mitigate risk, it should be fully and carefully implemented and verified. If it cannot be fully implemented due to design constraints, other methods of risk mitigation must be utilized.
12. NASA should expand existing data exchange and teaming efforts with other governmental agencies especially concerning age effects.

## **Introduction**

The Space Shuttle has four main propulsion elements. These are the Solid Rocket Boosters, the Space Shuttle Main Engines, the External Tank, and the Orbiter Maneuvering System and Reaction Control System.

The SIAT focused on issues associated with the Space Shuttle Main Engine. Several major issues were identified which have occupied most of the time and efforts of this task. The findings will be discussed in more detail in the body of this section of the report.

A top level review of the other propulsion elements did indicate other areas of concern that should be reviewed and assessed.

## **Assessment: Space Shuttle Main Engine**

### **Fleet leader process**

The fleet leader process for the Space Shuttle Main Engine ensures that no engine component, used for any flight engine, will ever be operated on a flight mission at greater than 50% of the life demonstrated during ground test at Stennis Space Center (SSC). The fleet leader test units are fired regularly at SSC to ensure that the all generic components always have a life margin equal to a greater than a factor of 2. If a component fails on a fleet leader test series, then all of the corresponding flight components on the entire fleet of flight engines are automatically replaced when they reach  $\frac{1}{2}$  this demonstrated life limit. The same fleet leader methodology is applied to any new or upgraded components after they are certified and introduced into the fleet. This process ensures a healthy, robust re-usable Space Shuttle Main Engine that will always have a life margin of 2 times the life demonstrated in hot fire ground test.

### **Foreign Object Debris (FOD)**

Foreign Object Debris was the main Space Shuttle Main Engine concern identified by the SIAT. The damage suffered to one engine nozzle during flight by an expelled Main Combustion Chamber liquid oxygen post deactivation pin is an example of one of the key events which caused the SIAT to be chartered. There have been other instances of foreign object debris throughout the program, accordingly, the SIAT intends to focus on the broad foreign object debris problem, including the liquid oxygen injector post de-activation pin issues.

There are two categories of foreign object debris which can cause engine damage: external and internal. Examples of potential external foreign object debris are gravel/debris impingement at engine start and loose Orbiter material. There has never been damage from on-pad objects due to the Kennedy Space Center diligence in keeping the pad clean, and loss and subsequent impact on the engine by the Orbiter drag parachute door has been precluded by design change. There do not appear to be further threats from external foreign object debris during flight. Rocketdyne has instituted an aggressive foreign object debris prevention program at Rocketdyne (Canoga Park), to preclude both external and internal foreign object debris during manufacture. They have created "FOD Free Zones" where all extraneous material is eliminated, and the only tools within the zone are needed for the assembly task being performed. Workers have been given extensive briefings and training relative to foreign object debris prevention.

The SIAT commends Rocketdyne for their in-factory foreign object debris prevention efforts. However, the treatment of internal Foreign Object Debris generated during engine operation or from routine in-process maintenance between flights requires an extensive review. The pin incident is a prime example of deficiencies in the system. All internal Foreign Object Debris occurrences during the program should be listed, with pertinent data on date of occurrence, material, and mass. The internal Foreign Object Debris FMEA/CIL's should be reviewed and the hazard categorized based on the worst possible consequence.



---

## Loss of LOX Post Pin

On the recent STS-93 flight there was a liquid oxygen low-level cutoff 0.15 seconds before the planned Main Engine Cut Off (MECO). This caused an Orbiter underspeed of 16 feet/ second, which was within the available margin required to achieve the planned orbit.

Both post-flight photos and real-time engine data indicated a nozzle fuel leak, which was confirmed after landing. Three of the 1080 nozzle coolant tubes were ruptured and showed evidence of impact damage (*Figure 10, Figure 11, and Figure 12*).

Tube leaks were confirmed after landing, with a calculated leak rate of  $4 \pm 0.5 \text{ lb}_m/\text{sec}$ , resulting in additional liquid oxygen consumption of  $\sim 5800 \text{ lb}_m$ . The nozzle leak was large enough to cause liquid oxygen low level cutoff.

Also, there was evidence of slight impact on the Main Combustion Chamber (*Figure 13 – Main Combustion Chamber Ding*) The Main Combustion Chamber damage was minor and no penetration of the coolant channels occurred.

It has been common practice to deactivate Main Injector Lox Posts, when they are determined to be life limited because of manufacturing or operational damage. When a post life limit is reached, a pin is inserted in the liquid oxygen post supply orifice (*Figure 14 – Powerhead, Main Injector and Liquid Oxygen Post Details*). The pin shuts off the liquid oxygen flow through the post, reducing high cycle fatigue loading. The tapered pin is about 1" long, 0.100 inches in diameter, gold coated, and is pressed with interference fit into the orifice.

There have been 212 pins used during the program, and 19 prior instances of pin loss during ground testing, with no impact damage. The practice was to insert the pin and perform a vacuum leak check. If there was no leak, an engine firing and subsequent successful vacuum leak check was required to ascertain that the pin would not be ejected. It is significant to note that 19 of 20 pins were ejected on the first engine firing. The one exception is E0220 which had a pin expelled after 31 hot fires. In November 1990, STS-38 was flown immediately after pin insertion. This practice was repeated for nine other pin installations on 5 STS missions before STS-93, with no pin loss.

The SIAT considers that a serious lapse in judgment and/or in attention to the engine data base occurred, which allowed two pins to be used in STS-93 without, ground test verification firing. The second pin was not ejected.

During the recent engine block changes (I & IIA), Main Injector manufacturing processes were improved to preclude liquid oxygen post damage. Currently, there are no pinned posts in the fleet. All future STS flights, starting with STS-103 are planned as either Block II or Block II-A Space Shuttle Main Engines. None of these engines have deactivation pins in any of the liquid oxygen injector posts at this time and it is not planned to fly any more pinned posts.

## Green Runs

New engines are acceptance tested to full mission duration before flight eligibility. Individual components which are new or have been overhauled are likewise tested (Green Run) on a development (non-flight) engine prior to use in the flight inventory. "Standard Repairs" such as liquid oxygen post deactivation are not necessarily tested before flight. The SIAT finds that there was pervasive evidence that liquid oxygen post pin insertion required a hot-fire verification. Of 19 pins ejected during ground testing, all but one were ejected during the first engine firing. The SIAT recommends comprehensive re-examination of maintenance and repair actions, for adequate verification requirements (i.e., visual, proof test, or green run) which require a pre-flight green run. Specifically, the SIAT feels that green run criteria need to be revised to increase mission safety and avoid future incidents such as the liquid oxygen post pin impact damage of the chamber wall tubes.

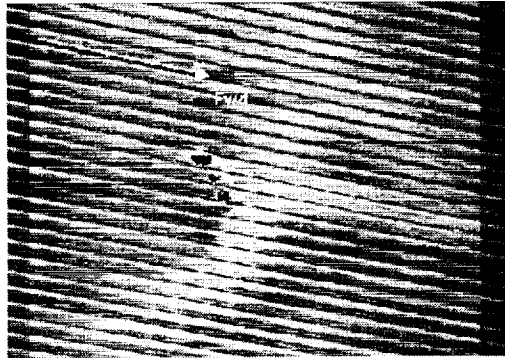
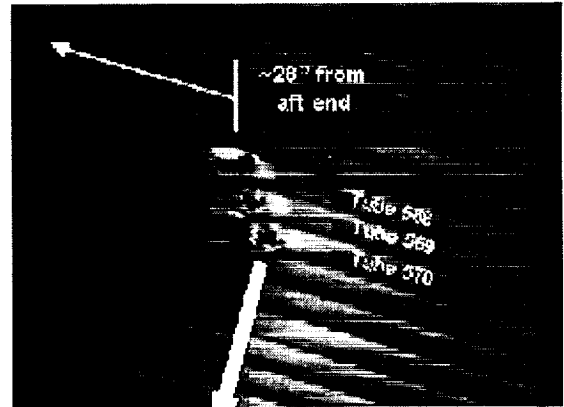


Figure 10 -- Ruptured Tubes, a



Dents noted at all  
3 tube ruptures.  
Evidence of gold present.

HOBO Myric Tube 570  
Hepublical tower

Figure 11 -- Ruptured Tubes, b

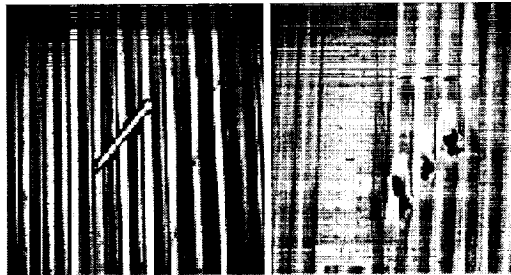


Figure 12 -- Ruptured Tubes, c

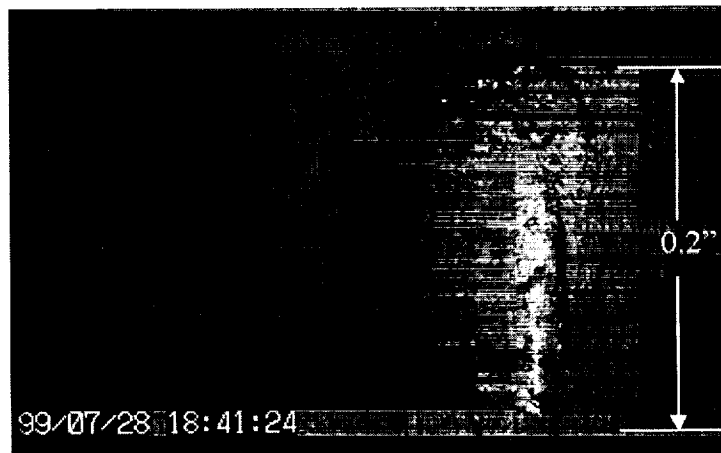


Figure 13 -- Main Combustion Chamber Ding

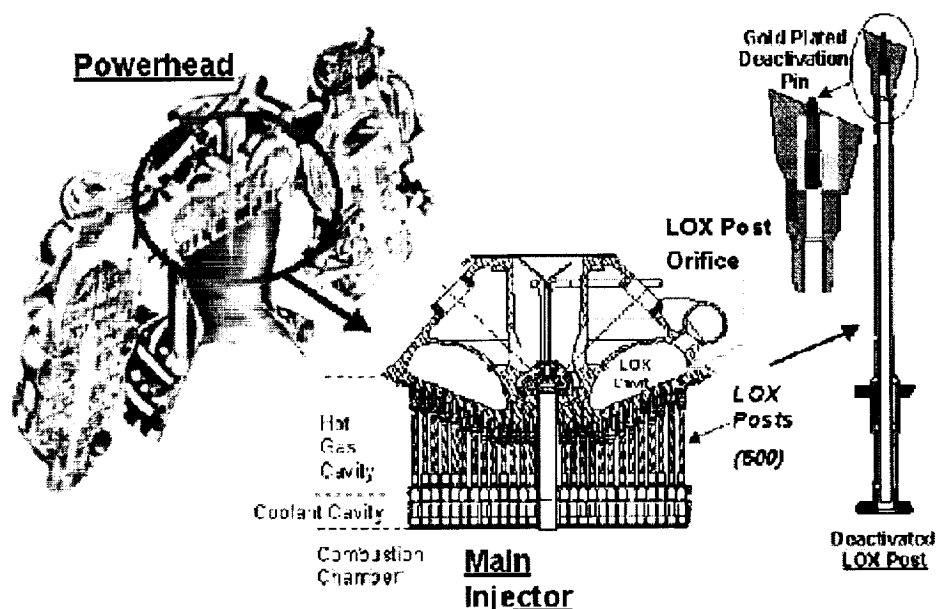


Figure 14 -- Powerhead, Main Injector and Liquid Oxygen Post Details

## Repairs

The SIAT believes that the handling of the pin insertion and test as a standard repair significantly contributed to the subsequent pin ejection and the nozzle damage during STS-93 flight. Its treatment as a standard repair precluded management visibility of the frequency of post deactivation and the evidence that hot-fire verification was integral to the repair process. Standard repairs are acceptable in some cases. The criteria for and the tracking of standard repairs and their FMEA/CIL's should be re-examined. The criticality of a standard repair should not exceed basic design criticality, based on worst case consequences, and all failures of standard repairs should be documented and brought to the attention of the Material Review Board. Furthermore any type of engine repair that involves hardware modification no matter how minor (such as LO2 post pin deactivation) should be briefed as a technical issue to the program management team at each Flight Readiness Review.

The SIAT hopes that as part of the new improved Block II A and Block II Space Shuttle Main Engine Main Combustion Chamber designs, there will be no further need to deactivate Main Combustion Chamber liquid oxygen injector posts. However, if the need to do so ever does occur again, a brand new non-friction lock dependent repair design/process needs to be developed and completely certified for any future affected engines. Furthermore it is strongly recommended that all future repair work of this nature (especially if there is any serious possibility of generating internal Foreign Object Debris as a result of the repair procedure) be fully reported and elevated to the SSP management team and especially during the Flight Readiness Review process. Treating these perceived to be lower level issues at a higher management cognitive level should certainly go a long ways towards preventing the type of liquid oxygen post pinning incident that resulted in a low liquid oxygen level premature engine shut down (and caused great public concern at the time) from occurring in the future.

## Processing/Discrepancy Reporting

The SIAT found that the low level of visibility of the history of pin losses greatly contributed to creating the opportunity for the STS-93 event. The basic systems for initial documentation of problems that are uncovered during Shuttle maintenance repair, refurbishment, and operations and then reporting these

problems up the management chain do not appear to be consistent, comprehensive, accurate, or well focused.

The top level problem data base which is intended to be the collection system and repository for all types of discrepancies, problem reports anomalies, manufacturing issues, etc, is the Problem Resolution and Corrective Action system. When this database was interrogated by the SIAT for specific samples of known problems, there were a number of omissions and ambiguities discovered within this information system. The example used was again the liquid oxygen post deactivation pin ejection problem on STS-93. This was declared to be an in-flight anomaly. A number of other pin ejection anomalies were reported to have occurred over the hot fire history of the Space Shuttle Main Engine family, both during ground test and once in flight. There was a history of 20 pin ejections verbally reported to the SIAT. However, when the Problem Resolution and Corrective Action database was sampled many of these anomalies could not be found in the system. Further more, other "pin ejection" problems were documented and reported that had not been described in the formal review presentations to the SIAT. These pin ejection anomalies turned out to be from a totally different functional application known as the liquid oxygen and fuel pump pre-burner injection "roll" or "support" pins used for an entirely different purpose than the liquid oxygen Main Injector post deactivation pin for the Main Combustion Chamber. This is one example of the ambiguity in the Problem Resolution and Corrective Action database that led to confusion as to which problem was being addressed. This ambiguity further complicates the process of reporting what could be critical Space Shuttle Main Engine flight readiness information up to the proper levels of management for determination of the flight worthiness of the hardware.

Another example of Shuttle information management breakdown is represented by the way in which the Main Combustion Chamber injector liquid oxygen pin repair was implemented and then reported up the decision making management chain as part of the Flight Readiness Review process for Engine Serial Number 2019 for STS-93. This breakdown is believed to be caused by the historical process for conducting Main Combustion Chamber injector liquid oxygen post deactivation pin repair work that was done in the early to mid 1970's prior to the first Shuttle flight in 1981. This liquid oxygen post pinning (a total of about 200 liquid oxygen posts for all engines to date) had always been done as a standard repair procedure derived from the standard repair specification and based on long standing historical precedent.

In spite of this long standing historical precedent, it is the opinion of the SIAT that the liquid oxygen post pinning of each Space Shuttle Main Engine injector should have been elevated to a level III Primary Material Review Board (PMRB) for each flight engine, as applicable. However, this was not the case for six separate flights (STS-38 through 93) for which the first "hot fire" of a newly pinned post was the flight engine burn during the actual mission. As part of this "casual" repair process the history of flight engine burns as a first post liquid oxygen pinning hot fire versus "green run" was not reviewed for each flight. The SIAT feels that six first time post-pinning hot fire flights on STS-38, 40, 42, 52, 56 and 75 had occurred prior to STS-93 should have been fully exposed and reviewed as part of the STS-93 Flight Readiness Review process. Again the SIAT strongly believes that instead of the limited visibility that was provided for the post pinning repair work and the associated reliance by the Space Shuttle Main Engine team on implicit rationale based on history, a specific technical issue briefing should have been given to the SSP management team during the STS-93 Flight Readiness Review.

## **High-Pressure Fuel Pump**

The SIAT views the completion of the Block II upgrades to be of high importance, as the High-Pressure Fuel Turbopump replacement is viewed as a significant safety improvement. The Alternate High-Pressure Fuel Turbopump has experienced delays due to problems encountered in certification. Upon completion of certification the Alternate High-Pressure Fuel Turbopump should be incorporated in the fleet as soon as possible.

## Assessment: Other Propulsion Elements

- Although there was no time for the SIAT to go into any real detail in these areas, there were other propulsion risk areas that were identified at the top level.

The external tank (ET) has a number of large cryogenic line mechanical joints requiring special seals to prevent leakage (especially in the main engine compartment at each of the engine inlets). In addition there are relief valves and vents to accommodate cryogenic boil off and to avoid over-pressurization. There is also concern about the overall structural integrity of the tank and certain manufacturing and repair processes such as welding of the lithium aluminum tank shell and domes. The structural integrity concerns also include the support and thrust load mounting struts. Another set of items that should to be received are the ground umbilicals and carrier assembly which represent a source of disconnect leakage at lift off after completion of topping operations.

Repeatability and quality of the grains in the Solid Rocket Booster motor segments may not be as thorough as it was in the earlier phases of the program. The SIAT is concerned that the quality control for these elements after the motor has been poured is a major potential risk area. The SSP should consider more frequent lot sample hot fire testing of motor segments at full-scale size to improve reliability and safety.

The whole lower case joint for the submerged nozzle of the Solid Rocket Booster including the hot gas seals, thermal barriers and flex joint/seal appear to be located in a very high thermal and mechanical stress zone. The concern for this design is exacerbated because the nozzle and associated joints are reused many times. The design and the post Solid Rocket Booster recovery inspection and re-certification for flight should be looked at and analyzed in careful detail by the SIAT.

The Thrust Vector Control power unit for the Solid Rocket Booster uses a hydrazine fueled gas generator to drive a turbine, which in turn drives the nozzle swivel joint hydraulic pump to achieve the desired Thrust Vector Control range. The use of a hydrazine system as the power source for this highly stressful environment (including parachuting into the ocean and subsequent recovery) reusable application is viewed as a high-risk situation for many reasons. Serious consideration should be given to replacing the hydrazine power unit with a safer and easier to maintain advanced electric auxiliary power unit for the Thrust Vector Control hydraulic unit. The same concerns apply to the hydrazine powered hydraulic Auxiliary Power Unit used on the Orbiter for various emergency and normal final landing hydraulic actuator functions (flaps, ailerons, elevons, etc).

In addition to the cryogenic mechanical joints between the External Tank and the Space Shuttle Main Engine inlets, there are a number of other cryogenic fluid mechanical joints that represent potential risks and should therefore be examined in detail.

There are three major hot gas mechanical joints inside the Space Shuttle Main Engine that represent potential leakage paths. These are the power head hot gas duets, the Main Combustion Chamber to power head joint and the Main Combustion Chamber to nozzle joint. Again, anything that would eliminate or improve the reliability of these joints would thereby enhance overall mission safety.

Both the Orbiter Maneuvering System and Reaction Control System hypergolic (i.e., earth storable) propulsion sub-systems on board the Orbiter represent, in the opinion of the SIAT, risk areas in several ways. The first observation of risk centers on the age of the hypergolic propulsion systems in the Orbiter fleet. Most of these systems have been in place and flight operational for more than 15 years. The feed systems are old and will probably be requiring more maintenance than in the past. These plumbing systems and the associated valving, regulators, etc. are often buried deep inside the Orbiter Maneuvering System and/or Reaction Control System feed system modules and are very difficult to access for maintenance and R&R. Not only is the hardware difficult to access, but all maintenance and/or repairs & refurbishment activities must be conducted by highly trained specialists who are protected at all times from the dangers of hypergolic propellants by being completely dressed in Self-Contained Atmospheric Protective Ensemble suits. These Self-Contained Atmospheric Protective Ensemble suits protect personnel very well but can inhibit manual dexterity and in tightly packed hardware situations with close fit ups, the Self-Contained Atmospheric Protective Ensemble helmets can impair the individuals peripheral vision. All of these constraints imposed by the mandatory use of Self-Contained Atmospheric Protective Ensemble suits can result in awkward and sometimes very difficult working conditions.

This problem is further exacerbated by the significant reduction in the last few years, of personnel comprising the maintenance crews at Kennedy Space Center that have had real experience (in depth) working with hypergolic propulsion equipment (including propellant draining, loading for flight and fluid component replacement). Improper handling of wetted hardware in the hypergol systems can cause spills of these caustic/corrosive liquids and vapors that could result in serious collateral damage to adjacent Orbiter flight hardware such as electrical cabling, electronic boxes, thermal protection materials (and the adhesives bonding the Thermal Protection System tiles in place), cabin windows and control equipment, as some examples. Unlike the other Shuttle propulsion elements (i.e., External Tank, Reusable Solid Rocket Motor/Solid Rocket Booster and Space Shuttle Main Engine) where all the equipment/hardware is maintained or replaced by the OEM's, the reduction of experienced personnel over the last few years has resulted in no OEM personnel being involved in any of the hypergolic propulsion maintenance and operations. The Orbital Maneuvering Engine was produced and manufactured by Aerojet who has not been involved for more than 10 years, while their original, high performance storable propellant engines have been aging over the last 18 years. Similarly, the reaction control engines were manufactured by the Marguardt Corp who has not only been out of the loop for a number of years but who has changed management multiple times as they were sold and resold over these years.

Finally, the Orbiter Maneuvering System and Reaction Control System pod feed systems were originally integrated by the old Rockwell Corporation (North American Aviation) using purchased fluid components from in some cases, now defunct suppliers and tanks from McDonnell Douglas, St. Louis (Orbiter Maneuvering System) and Martin, Denver (Reaction Control System). Since that time, of course, Boeing has taken over the Orbiter program and most of the day-to-day operations and maintenance work is being done by even less experienced people at USA.

Against this background, it was reported to the SIAT that it is planned to modify the system to add cross feed lines between the forward and aft Orbiter Maneuvering System and Reaction Control System pods, through the mid-body or one of the wings. It was also described that additional plumbing was to be added, as well, including quick disconnects so that the whole modified Orbiter hypergolic propulsion system could be used to re-fuel the Space Station (ISS) propulsion modules with residual propellants from the Orbiter. All of this adds to the risk concerns already expressed by the SIAT for this propulsion element.

There is also a concern for the electrical heating system used to maintain the hydrazine for the Auxiliary Power Unit and HPU at safe temperatures with adequate safe margins (heater failures, on or off could result in very serious line ruptures, fires and/or explosives). While the heaters are fully redundant, the heater power lines tie back to a single point at the power source bus bar. A failure at this single point could definitely result in some serious problems during the Orbiter flight mission.

## Summary

The propulsion elements of the Shuttle are by nature high risk. While many processes are in place to mitigate these risks, most notably Fleet Leader testing, it remains imperative that all maintenance and operation procedures adhere to rigorous requirements for repairs, verification testing, and problem reporting. The recent main engine post pin ejection incident indicates a breakdown in these procedures that has serious potential impacts on flight-safety. This and other deficiencies must be corrected as described in the findings and recommendations listed above.

## Risk Assessment & Management

### Findings

1. Flight Safety Risk Reporting at the Program Management level may be either optimistic or inaccurate. This results from a process that is based primarily on qualitative and often subjective methods (e.g., risk matrix). The lack of statistical and quantitative risk assessment tools in the SSP results in the limited ability to measure and control risk.
2. Although it is clear that the SSP has extensive requirements and procedures in place to assure flight safety, the SIAT believes based on SSP input that a program-wide risk management plan that defines and integrates the risk management activities across all the Shuttle elements is lacking. The result is the inconsistent and non-uniform use of risk management tools.
3. Failure analyses and incident investigations are sometimes limited to a subset of all the possible causes rather than based on a comprehensive fault-tree approach to identify the root cause.
4. A periodic review of maintenance procedures, waivers, and incidents is not feasible without an accurate historical database. PRACA has deficiencies that preclude its effective use as a decision support tool.
5. The actual safe life of some systems may be masked by the lack of a comprehensive age management program. If the actual life is less than the assumed life, an increase in risk is unknowingly assumed.
6. The SSP places undue reliance on system redundancy and abort modes to mitigate risk.

### Recommendations

1. The SSP should revise the risk matrix for probable and infrequent likelihood for CRIT 1R\*\* and 1R\* severity to require a greater level of checkout and validation.
2. Risk assessment matrix and Failure Modes and Effects Analysis should be updated based on flight failure experience, aging and maintenance history, and new information (e.g., wiring, hydraulics, etc.).
3. The SSP should explore the potential of adopting risk-based analyses and concepts for its critical manufacturing, assembly, and maintenance processes, and statistical and probabilistic analysis tools as part of the program plans and activities. Examples of these analyses and concepts are Process FMEA/CIL, Assembly Hazard Analysis, Reliability Centered Maintenance, and On Condition Maintenance.
4. NASA, USA, and the SSP element contractors should develop a Risk Management Plan and guidance for communicating risk as an integrated effort. This would flow SSP expectations for risk management down to working level engineers and technicians, and provide insight and references to activities conducted to manage risk.
5. Failure analysis and incident investigation should identify root cause and not be artificially limited to a sub-set of possible causes, e.g., wiring.
6. Prior to every flight, the SSP should review all waivers or deferred maintenance to verify that no compromise to safety or mission assurance has occurred.
7. The SSP should revise the Problem Resolution and Corrective Action database as recommended in the **Problem Reporting & Tracking Process** section.
8. A formal Aging and Surveillance Program should be instituted.
9. Where redundancy is used to mitigate risk, it should be fully and carefully implemented and verified. If it cannot be fully implemented due to design constraints, other methods of risk mitigation must be utilized.

10. Standard repairs on CRIT1 components should be completely documented and entered in the Problem Resolution and Corrective Action system.
11. The criteria for and the tracking of standard repairs, fair wear and tear issues, and their respective FMEA/CIL's should be re-examined.
12. The SIAT recommends comprehensive re-examination of maintenance and repair actions for adequate verification requirements (e.g., visual, proof test, or green run).
13. An independent review process, utilizing NASA and external domain experts, should be institutionalized.
14. The SIAT believes that Aerospace Safety Advisory Panel membership should turnover more frequently to ensure an independent perspective.

## Introduction

Risk management is a critical part of the overall management process and an integral part of program management. It provides the processes necessary to identify potential issues and permit mitigation techniques to be determined and implemented. Timely and effective risk mitigation provides a program with high levels of safety, enhanced probability of mission success, improved availability/supportability of the system, and reduced schedule and cost risk.

Recent events that have occurred on the Orbiter Discovery (OV103) in preparation for flight caused the SIAT to focus on and review the current Space Shuttle Program (SSP) risk management program. This summary report is prepared in support of the SIAT. It is intended to evaluate the Space Shuttle Program (SSP) risk management practices, identify any issues and concerns, and make recommendations for improvement.

SSP requirements contained within NSTS 07700 provide definition and process requirements for the identification, analysis, and control of hazards within the Space Shuttle Program. All SSP Contractors are contractually required to conduct and submit FMEA/CIL and Hazard Reports for Program approval. All submittals require review by the System Safety Review Panel prior to SSP acceptance (see also **Appendix 8**).

## Assessment

There is no doubt that the risk management practices embedded in the documents and procedures discussed in the **SSP Risk Management Process** sub-section in **Appendix 8** constitute a very extensive effort to maintain high level of Shuttle flight safety. However, there are some issues and concerns that the SSP must address to manage and continue its strong safety record. The main issues can be summarized as follows.

### **Lack of Standard Statistical and Quantitative Risk Assessment Tools**

The SSP relies primarily on qualitative tools to assess and manage risk. The most important qualitative tools that SSP uses are the FMEA/CIL and hazard analyses. Failure Modes and Effects Analysis is a "bottom-up" approach used to identify the potential failure modes and their effects. Hazard analysis is a "top-down" approach to identify undesired scenarios and their causes and effects. Both tools have a proven history in identifying risk. However, they are qualitative in nature and not designed to prioritize risk.

Since the Challenger accident in 1986, quantitative probabilistic and statistical tools have been used to a limited extent by the Shuttle program. Although not part of the SSP requirement, these tools have been used informally to support the qualitative tools in place and have been effective in managing the risk of the Space Shuttle critical hardware. One example is the Single Flight Reliability (SFR) criterion used by the Space Shuttle Main Engine element, that allows the SSP to extend the life of selected SSME critical hardware based on an increase in the level of statistical confidence generated by additional test data as they are accumulated. Statistical Process Control (SPC) is another statistical tool that has been used by some of the SSP elements, for example, in controlling the process variability in some of the Super Light Weight Tank (SLWT) and the Reusable Solid Rocket Motor critical processes. Reducing and controlling process variability translate to reducing and controlling risk.



---

Another effective tool that the SSP has used is the Fault Tree Analysis (FTA). This tool can be used in both a quantitative and qualitative manner. It also can be used in proactive (what can go wrong) and reactive (what went wrong) modes. The SSP has used this tool qualitatively in problem investigations, anomaly dispositions and in the analysis of Flight Hazard Reports.

One major probability-based quantitative risk assessment tool that NASA has been trying to develop and implement in the SSP is the Probabilistic Risk Assessment (PRA) tool. Since 1987, several efforts have been made to establish a Probabilistic Risk Assessment model for the SSP similar to models established for nuclear power plants. The most extensive one is the Quantitative Risk Assessment System (QRAS) modeling effort, which is being conducted by NASA and the Shuttle prime contractors. The Quantitative Risk Assessment System is still in the development stage and is not certified (although it has been effectively used in evaluating Shuttle upgrades). Therefore, the current Quantitative Risk Assessment System model should be used with caution. It should mainly be used for risk prioritization and as a source of Shuttle failure rate data with less emphasis on the absolute numbers. The lack of good models for human/process reliability and common cause failures similar to those that exist for the nuclear power industry could constitute significant limitations of the Quantitative Risk Assessment System model. Other limitations could include the incomplete modeling of some risk contributors such as aborts, CRIT 1R, and some sub-system interfaces.

It is apparent to the SIAT that the SSP has not formally incorporated statistical and quantitative methods into its risk management process. Tools are used primarily to identify risk; a rigorous, analytical evaluation of risk is typically not made. An example of this lack of quantitative analysis is in the history of LOX pin ejection. Partially due to a lack of data, the probability of a liquid oxygen pin ejection was never updated to account for the 19 pin ejections that happened over a space of several years (see **Problem Reporting & Tracking Process**). The many liquid oxygen pin ejections should have changed the risk probability to 1 in 10 and required a checkout at each phase. No effort was made to look at similar systems where pins were utilized or to update the component risk probability and assessment. This lack of statistical risk assessment is almost cultural; the SSP team seems confident that once the risk has been identified and a cursory probabilistic assessment performed, little or no attempt is made to look at probability data from SSP failures or incidents to see if the risk assessment is accurate (to the SIAT's knowledge).

### **Lack of Overall SSP Risk Management Plan**

As part of the Space Flight Operations Contract (SFOC), NAS9-20000, NASA has a contractual requirement for USA to develop and implement a risk management plan<sup>10, 11, 12</sup>.

In response to this requirement, USA developed the Space Shuttle Program Risk Management Plan (SFOC-PG9604).<sup>13</sup> Currently, a new plan (SFOC-PG9604-Rev.A) is being reviewed for approval by the SSP. There are no procedures in place for SSP contractors to implement the current plan, although it is used as part of the USA infrastructure to support the Certificate of Flight Readiness process. Preliminary evaluation revealed that the plan does not take advantage of the quantitative tools that NASA has developed and used in the risk assessment area since the Challenger accident.

Risk management efforts are hampered by this lack of a program-wide risk management plan. Even though several specific documents exist which define the role of risk management in critical flight safety areas, the use of assessing critical risk definitions is often left up to individual engineers, often with inconsistent results. Specific deficiencies are:

#### Lack of risk assessment on critical decisions

The SIAT noted that the decision to defer both depot and post landing maintenance were done with minimal if any risk assessment. Even though the SIAT recognizes that it is sometimes necessary to defer rework of non-critical deficiencies in order to meet schedule, these deferred items should be thoroughly reviewed to determine the impact on mission operations and safety of flight. It was stated by the SSP that the Program Review Change Board addresses all waivers and deferred maintenance; however, this review process was not clear to the SIAT. Furthermore, it appeared that once granted, waivers were rarely re-examined or removed; the SIAT was alarmed to learn that more than 500 waivers existed on STS-93, many in existence since 1988.

The creation of a "fair wear and tear" specification was utilized to allow a relaxation of Shuttle maintenance to account for the normal wear associated with Shuttle operations. Even though it is impracticable to expect a twenty year old launch vehicle to have the identical performance to a new system, the creation of this specification was done with only engineering judgement without any formal risk assessment process. It is the opinion of the SIAT that the creation of this specification may have contributed to the relaxing of standards by technicians, quality assurance and engineering personnel. This acceptance of some amount of damage may have contributed to the wiring problems discovered during STS-93. At a minimum, the acceptance of wear had the potential to increase the probability of risk and should have been cause for review.

#### Lack of Program Risk Communication Guidance

In conjunction with risk assessment requirements and tools, a standard policy needs to be generated which provides detailed guidance on what decisions and risk analysis need to be briefed at what level. Most of the decisions to approve a waiver for deferred maintenance were left up to the working level engineer with only a cursory review by SSP management. Because waivers have been previously approved and documented during the PRCB process, they are not briefed at the FRR. However, the SIAT believes this procedure makes the risks accepted for launch invisible to SSP managers in their decision-making process.

Critical reviews like the Flight Readiness Review and the Pre-Launch Assessment conducted by Safety and Mission Assurance (see **Safety and Mission Assurance**) need to focus attention on critical information and not get distracted by low importance details. When queried about how the SSP management reviews critical waivers to make sure that safety and mission success are not being compromised, the SSP responded that no summary charts are generated and that detailed information is available in the Problem Resolution and Corrective Action database. A better risk communication plan forces review at each level so that top level management is not forced to sift through reams of data looking for relevant, important information.

### **Inaccurate Reporting of Flight Safety Risk**

The SIAT is concerned that risk is understated (i.e. low) for "probable" likelihood of CRIT 1R\*\* and 1R\* severity occurrences (see **Appendix 2**), i.e., acceptance of single failure tolerant condition requires "Validation Each Flow and Checkout at Intervals" and "Checkout Each Flow." This situation, coupled with concerns over deferred maintenance actions, waivers, open CRIT 1 Corrective Action Records, etc. can mask the true safety risk presented at Program and Flight Readiness Reviews. A similar condition may exist for "infrequent" likelihood. In contrast to some opinions in NASA, the SIAT believes that the risk management system does not afford Shuttle program officials the opportunity to comprehend the scope and extent of safety critical deferrals and waivers (e.g., 3 weeks prior to the launch of STS-103, 89 CAR's, 8 with CRIT levels of 1 or 1R, remained open; see also **Appendix 11**). Since the Shuttle design does not provide redundancy for all critical failures, risk categorization, assignment, and comprehension are the most important elements of the Shuttle safety program.

### **Incomplete Failure Analyses and Anomaly Investigations**

One of the ground rules of any failure or mishap investigation is the evaluation of all potential causes of the failure, and then the subsequent elimination of potential causes by analysis. The wire short on STS-93 was caused by the breakdown of the wiring insulation which was characterized by the SSP team as "ringing" or a circular cracking of the insulation. The SSP engineering team performed testing and determined that aromatic polyimide insulation was susceptible to cracking when a notch in the insulation was then subjected to flexing. Once this failure mode was verified, the incident investigation was limited to possible causes that could either induce a notch in the insulation or cause extreme bending (i.e. maintenance).

The breakdown in the incident investigation was that, to the best of the SIAT's knowledge, no one ever considered that there may be multiple problems which lead to a "ringing" of aromatic polyimide insulation. Despite years of experience with age related problems with aromatic polyimide insulation in both the US Navy and Air Force, no attempt was made to investigate either hydrolysis or contamination to high pH fluids as a potential source of the "ringing". This narrow focus has the potential to artificially limit the investigation and cause critical risks to be overlooked.

One of the better efforts to communicate technical information is through the Joint Aeronautical Commander's Group (JACG) which NASA participates. The Aging Aircraft Program has expanded initial efforts concerning structural systems to include wiring, avionics and other non-structural systems. Despite this arrangement, NASA and USA engineers seemed unaware of recent investigations and concerns over aircraft wiring and avionics obsolescence management. This lack of information has the potential to mask critical high risk deficiencies.

### **Inaccurate Historical Database**

Deficiencies in the Problem Resolution and Corrective Action data system have been thoroughly documented in the **Problem Reporting & Tracking Process** section of this report. Several deficiencies are also discussed here because they contribute to a false sense of security and adversely impact corrective actions. The Problem Resolution and Corrective Action system needs to be more than a historical repository of data; it needs to be a real time system that can alert working level engineers and managers of *potential* problems long before an incident occurs. The current system is not able to adequately check trends in overhaul or manufacture to establish trends prior to launch preparation nor does it provide data and analysis to support both the individual engineer and management. The system needs to provide data to the avionics engineer at Kennedy Space Center and to the wiring engineer at USA to ensure that adverse trends are not causing an increase in risk to their system.

### **Summary**

Despite the extensive requirements and procedures in place to assure flight safety, deficiencies exist in the current Space Shuttle risk management system. Integration and centralization of Risk Management processes are needed to provide additional focus on the importance of this proactive activity. Consolidation of the various SSP risk management activities into a single risk management plan that defines and integrates the risk management activities across all the Shuttle elements needs to be considered. The SIAT recommends that S&MA move away from its current role as "auditor" and return to a more proactive oversight role which selectively performs independent investigations of trends and assessments of risk (see **Safety and Mission Assurance**).

In the analysis area, the SSP should expand its risk based analysis capability including numerical probability-based analysis. As with any analysis process, the value of accurate and usable databases cannot be overstated. The Problem Resolution and Corrective Action database is inadequate and difficult to use. The SSP should improve the Problem Resolution and Corrective Action database quality and analysis capability in order to perform trending and quantitative risk analysis (see also **Problem Reporting & Tracking Process**).

## Safety and Mission Assurance

### Findings

1. The Safety & Mission Assurance community made little input and had little visibility to the SIAT. In contrast, quality assurance personnel were very accessible to the SIAT and provided considerable input.
2. The degree of independence of the Safety & Mission Assurance reporting chain was difficult to assess.
3. The transition from oversight to insight has resulted in the loss of critical information for the decision-making process. A reduction in Safety & Mission Assurance oversight and functions is not commensurate with the "one strike and you're out" environment of Shuttle operations. Similarly, a reduction in surveillance by NASA quality assurance adversely affects mission and flight safety.
4. Investigation of recent in-flight anomalies and current program documentation indicate possible process breakdowns and/or deficiencies in the Safety & Mission Assurance function. This finding is reinforced by the significant number of escapes/diving catches reported by NASA Quality (see **Appendix 3**), and the "stumble-on" problems reported by United Space Alliance<sup>14</sup>, and indicates the need for improvements in Mission Assurance processes and quality assurance surveillance procedures.

### Recommendations

1. The current quality assurance program should be augmented with additional experienced NASA personnel.
2. The SSP should review all waivers or deferred maintenance to verify that no compromise to safety or mission assurance has occurred.
3. NASA and USA quality inspection and NASA engineers should review all CRIT 1 system repairs.
4. NASA Safety and Mission Assurance surveillance should be restored to the Shuttle Program as soon as possible.
5. The Safety & Mission Assurance role should include: mandatory participation on Prevention/Resolution Teams and in problem categorization, investigation of escapes and diving catches (see **Appendix 3**), and dissemination of lessons learned.

### Introduction

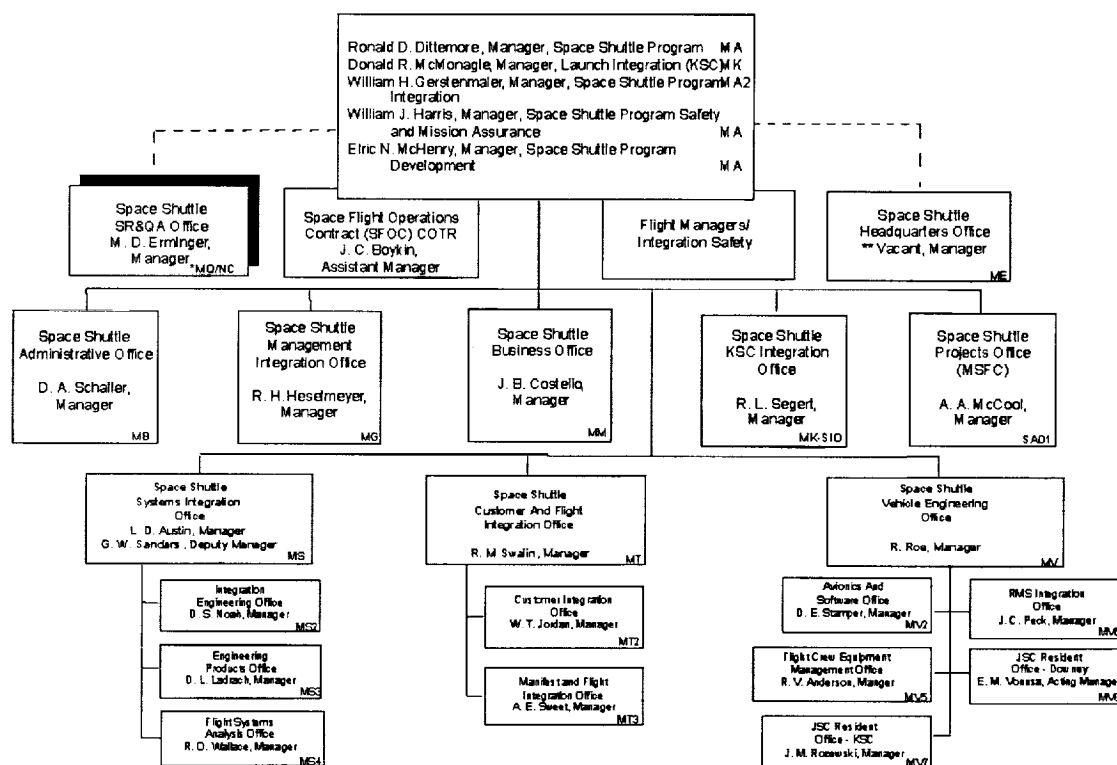
The SIAT believes strongly that an independent, visible Safety and Mission Assurance function is vital to the safe operation and maintenance of the Shuttle. The Shuttle program in its "one strike and you're out" environment is unlike most other defense or commercial industries. As a consequence, it is believed the industry trend toward reducing Safety & Mission Assurance oversight and functions is inappropriate for the Shuttle. Further, the SIAT fully endorses the Rogers Commission<sup>15</sup> view that the Safety & Mission Assurance function should possess both organizational and reporting independence. With this perspective, the SIAT paid particular attention to the Safety & Mission Assurance function in briefings by the Shuttle program to assess its role and responsibilities in Shuttle processing and maintenance.

### Assessment

The organizational position of the Safety & Mission Assurance function has important implications for its autonomy: too much dependence on management to act on the problems and recommendations brought forward by the Safety & Mission Assurance community can compromise the effectiveness of the Safety & Mission Assurance role and perspective. Review of the Shuttle program organization shows that the NASA Shuttle SM&A

## SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT

function sits outside the program and reports to the Center Director at Johnson Space Center. However, there is an indirect line of reporting from the Shuttle Safety & Mission Assurance manager to the Shuttle Program Manager, as shown in *Figure 15 – Safety, Reliability, & Quality Assurance Interface to SSP Office*. The USA Safety & Mission Assurance function directly reports to USA Shuttle operations managers. This overall organization is unchanged by the introduction of the Shuttle Flight Operations Contract. At Marshall Space Flight Center the reporting chain, shown in *Figure 16 – Marshall Space Flight Ctr. S&MA Reporting Interfaces*, has the Safety & Mission Assurance reporting to the Space Shuttle Projects Office and to HQ through the SSP Safety, Reliability and Quality Assurance office at Johnson Space Center. The Safety & Mission Assurance community does conduct a Pre-Launch Assessment Review with representatives from Johnson Space Center, Kennedy Space Center, Marshall Space Flight Center, and HQ in preparation for signing the Certificate of Flight Readiness.



**Figure 15 -- Safety, Reliability, & Quality Assurance Interface to SSP Office**

There also exists an overall independent assessment function group at Johnson Space Center which reports directly to the Associate Administrator-OSMA concerning Shuttle safety issues. So it appears that independent reporting paths are accessible to the Safety & Mission Assurance function; however, because of indirect reporting chains to the Program, it is difficult to ascertain the degree of this independence.

It is apparent that NASA Safety & Mission Assurance is moving away from an oversight role to one of insight, in which direct involvement is being replaced by periodic surveillance and audits. This move may result in fewer independent reporting paths as the NASA presence is withdrawn from engineering and operations teams. It may also reduce the ability of the Safety & Mission Assurance function to determine and enforce compliance to safety and reporting requirements. Further, in an "insight" role, Safety & Mission Assurance will become, by definition, more reactive than proactive. These concerns are corroborated by the November 1996 Aerospace Safety

Advisory Panel report, which cites that "periodic independent assessment activities, audits, and analyses of metrics are not sufficient to provide the degree of independent safety oversight required to operate the Space Shuttle program at minimum risk levels in the absence of a NASA physical presence on the floor."

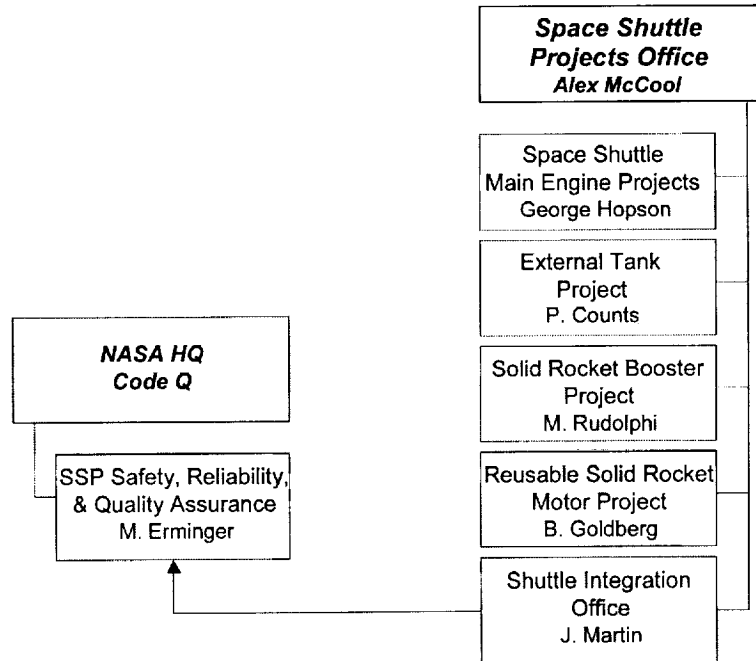


Figure 16 -- Marshall Space Flight Ctr. S&MA Reporting Interfaces

As the duties of the Shuttle Safety & Mission Assurance organization have been reduced, so too has its workforce. At Marshall Space Flight Center, the Safety & Mission Assurance support contractor level was reduced from 150 to 80 in 1995 and activities such as statistical trending of Space Shuttle Main Engine problems were eliminated. A reduction of workforce may also lead to a reduction in capabilities as expertise and experience are lost. This concern has been also voiced by the Aerospace Safety Advisory Panel, which found: "The long term maintenance of independent safety oversight will require NASA to develop and implement programs for critical skills retention and for the generation of direct Space Shuttle operating experience among NASA employees."

Shuttle Safety & Mission Assurance still has responsibility to perform trending and recurrence control, risk assessments of requirements changes and of problem resolutions, and criticality analyses. It is also the responsibility of Safety & Mission Assurance to brief FMEA/CIL's and hazards that are new or of increased risk to Program Management for upcoming flights. Consequently, it is of concern to the SIAT that Safety & Mission Assurance did not directly brief the SIAT and had little visibility throughout the assessment. Of greater concern is that the performance of Safety & Mission Assurance duties appears to be diminishing.

The Main Injector pin ejection anomaly (STS-93) demonstrates deficiencies in trending and recurrence control and in the risk assessment of the problem resolution (in this case a standard repair). Deficiencies in risk assessment of requirements changes is indicated in the current number of wiring anomalies; the classification of fair wear and tear allowances on wiring integrity was too loose. And finally, the SIAT is concerned about how well the status of FMEA/CIL's are communicated to Program Management. For STS-93 alone, 330 waivers of CIL requirements existed, some granted as early as 1988. CIL waivers include acceptance of hardware not meeting redundancy or fail safe requirements and the addition of newly discovered failure modes. The number and age of these waivers suggest to the SIAT that a breakdown in the process of criticality monitoring and risk communication may have occurred.

There are several areas in which the SIAT feels the role of Safety & Mission Assurance should be expanded. The first is in the investigation of anomalies, escapes, diving catches, and other escapes (see **Appendix 3**). The SIAT feels that each of these types of occurrences should be investigated independently by Safety & Mission Assurance to promote complete and unbiased discovery and reporting. Secondly, it is believed that Safety & Mission Assurance should take a larger role in the compilation and dissemination of lessons learned. The current process for distribution of lessons learned across systems and sub-systems (i.e., wiring damage) appears to be inadequate. And finally, the SIAT believes that Safety & Mission Assurance participation on Prevention/Resolution Teams that have responsibility for problem resolution and recurrence control should be mandatory and that Safety & Mission Assurance should review all problems and their designation as in- or out-of-family. The Aerospace Safety Advisory Panel similarly recommends that "NASA should evolve its independent safety oversight efforts into a system in which it receives notification of *all* changes, anomalies, and re-certifications from the Shuttle Flight Operations Contract contractor."

## Summary

Recent reductions in duties and personnel have resulted in a Safety and Mission Assurance process that appears largely absent from day-to-day activities of Shuttle operations and maintenance. Further, the deficiencies observed in risk assessment, risk communication and problem trending, and the increasing occurrences of "stumble-ons," "diving catches" and "escapes" indicates degradation in the Safety & Mission Assurance system that remains. The SIAT strongly believes in the necessity of an experienced, well-staffed NASA quality assurance function ("second set of eyes") and an independent, empowered NASA Safety & Mission Assurance function ("third set of eyes"). Listed above are detailed findings and recommendations that the SIAT believes will help achieve these standards.

## Software

### Development & Maintenance

#### Findings

1. An in-depth review of software systems was not possible in the time available. However, as the SSP has very strict controls on software changes and updates, the SIAT has not been made aware of any issues that affect flight safety.
2. Imminent system upgrades and replacement (e.g., glass cockpit, GPS, ISS interfaces) will require extensive modifications and additions to software.
3. Current philosophy and staffing levels may not be adequate to accommodate anticipated upgrades. Implementation will require increased resources and carefully analyzed tradeoffs.

#### Recommendations

1. The SIAT believes that software systems (flight, ground, and test) deserve a thorough follow-on evaluation.
2. Software requirements generated by Shuttle system upgrades must be addressed.
3. Enhanced software tools should be considered for potential improvements in reliability and maintainability as systems are upgraded.

#### Introduction

The assessment of software development and verification was based upon briefings with the Shuttle Program IV&V team. The process through which flight software is developed and maintained was examined in detail and is described in **Appendix 9**.

#### Assessment

##### Flight Software Process

After multiple conversations with personnel from Johnson Space Center and the Independent Validation & Verification facility, all agreed that current interactions between the SSPO and the Independent Validation & Verification facility in West Virginia are excellent. No specific recommendations or issues were identified to improve or change the current process.

The multiple steps currently included in the process serve as gatekeepers to ensure that the process does not progress prematurely. The practice of including actual mission hardware, e.g., Line Replaceable Units during the Shuttle Avionics Integration Laboratory testing, has identified problems at a stage when they could be resolved with no impact to mission or personnel safety.

##### Shuttle Avionics Upgrade

As the Shuttle Development Program (Upgrades) progresses, clearly defined requirements and careful decisions will be required to make necessary tradeoffs. It is imperative that the SSPO carefully weigh the



tradeoffs that could be made using proper risk management technology and processes. Increased funding will be required to support both the upgrades and the operational maintenance efforts; tradeoffs without increased resources in this area will likely add undue risks to the program and crew.

### **Enhanced Tools**

Although no specific tools were mentioned, research methods are making new automated development tools available. These should be explored for potential improvements in reliability and maintainability as avionics systems are upgraded and enhanced.

### **Summary**

No flight safety issues were identified for Shuttle software systems during this assessment. However, due to time and resources limitations, the SIAT was not able to evaluate this area as strenuously as desired. Consequently, as recommended above, the software validation and verification process for existing as well newly developed systems should be scrutinized.

## Structures

### Airframe, Thermal Protection Systems, and External Tank

#### Findings

##### Orbiter Structure

1. The SIAT believes the number of NASA Quality Assurance personnel inspecting the Orbiter structure is insufficient.
2. Recent occurrences of problems and quality relative to Orbiter structural and mechanical components indicate systemic issues may exist in the maintenance process, particularly in areas of workmanship and inspection verification. This finding is substantiated by the many “stumble-ons” and escapes reported by United Space Alliance<sup>14</sup> following Orbiter structure maintenance and inspection.
3. Current Shuttle practices for aging structures and components are inadequate and do not reflect lessons learned from the recent world-wide aging aircraft studies.
4. The analyses upon which current structural fatigue lives and inspection intervals are based use non-conservative estimates of fatigue crack growth thresholds.
5. Potential for hydrogen assisted sustained load cracking in the Shuttle main engine high-pressure fuel lines and valves is high.

##### Non-Destructive Evaluation and Maintenance

1. Current inspection technique(s) for locating fatigue cracks and corrosion under the tiles or in inaccessible areas may not be adequate, and therefore can not ensure the integrity of primary structures.
2. The similarities between the aging commercial fleets and the small Shuttle fleet warrant new assessments based on these new understandings in the areas of non-destructive inspection and maintenance.

##### Corrosion

1. Areas where corrosion damage has occurred on the Orbiter were not anticipated in the original design.
2. Where corrosion was anticipated, existing corrosion prevention systems are degrading with age.
3. Inspection is the primary strategy used to identify and control corrosion. Hidden corrosion needs a proactive inspection program with practical and reliable NDE techniques.
4. Corrosion will accelerate with age and must be considered in structural integrity analyses. In inaccessible areas, worst case pitting depth and area loss must be assumed.

##### Thermal Protection Systems

1. The thermal protection system (TPS) is very sensitive to process changes; it requires a high level of quality control to keep a functional system and find imminent problems

2. Past improvements to the thermal protection system are commended and demonstrate a successful corrective action program.

### **External Tank**

1. The SIAT is concerned with the inspection and proof-test logic used to screen for flaws or cracks in the Super-Light-Weight Tank in light of the reversal in fracture-stress-vs.-flaw-size at room and cryogenic temperatures.

### **Recommendations**

1. The current quality assurance program should be augmented with additional experienced NASA personnel.
2. The criteria for and the tracking of standard repairs, fair wear and tear issues, and their respective FMEA/CIL's should be re-examined.
3. NASA and USA quality inspection and NASA engineers should review all CRIT 1 system repairs.
4. The SIAT recommends comprehensive re-examination of maintenance and repair actions for adequate verification requirements (e.g., visual, proof test, or green run).
5. NASA should expand existing data exchange and teaming efforts with other governmental agencies especially concerning age effects.
6. A formal Aging and Surveillance Program should be instituted.
7. An assessment of using lower fatigue-crack-growth thresholds and their impact on fracture critical parts or components needs to be reviewed to establish life and verify the inspection intervals. Retardation and acceleration model(s) should be used to assess the type of crack-growth history under the Orbiter spectra.
8. Assessments of the impact of any new Orbiter flight loads on structural life should continue as responsibility for the Orbiter structure is transferred to the contractor.
9. Inspection technique(s) for locating corrosion under the tiles and in inaccessible areas should be developed.
10. Hidden corrosion problems require a proactive inspection program with practical and reliable non-destructive evaluation techniques; at this point, this inspection is done on a randomized basis. An assessment of the impact of hidden (or inaccessible) corrosion and the repairs of identified corrosion on the integrity of the Orbiter structure should to be made.
11. The Orbiter Corrosion Control Review Board should consider incorporating the framework suggested by the Federal Aviation Administration for Corrosion Prevention and Control Plans of commercial airplane operators into their corrosion database to provide focus to the more serious occurrences of corrosion.
12. The inspection and proof-test logic to screen for flaws or cracks in the Super-Light-Weight Tank should be reviewed in light of the reversal in fracture-stress-against-flaw-size between room and cryogenic temperatures.
13. The design and the post Solid Rocket Booster recovery inspection and re-certification for flight should be looked at and analyzed in careful detail by follow-on independent reviews.
14. Standard repairs on CRIT1 components should be completely documented and entered in the Problem Resolution and Corrective Action system.
15. The inspection procedures of the Shuttle main engine high-pressure fuel lines and valves to find cracks should be reviewed. Currently, Columbia is at Palmdale and the vehicle is available for inspection of the main propulsion system lines to verify whether this potentially serious problem exists.
16. Where redundancy is used to mitigate risk, it should be fully and carefully implemented and verified. If it cannot be fully implemented due to design constraints, other methods of risk mitigation must be utilized.

## Introduction

A technical meeting was held at the NASA Johnson Space Center on the Orbiter Airframe Structure and Thermal Protection Systems to augment information obtained during formal SIAT meetings. The lessons learned on the recent aging aircraft programs conducted by the aircraft industry and the Government were assessed relative to the Shuttle structure. This assessment covers the Orbiter structure, the non-destructive evaluations (NDE) and maintenance, corrosion, and the thermal protection system of the Orbiter.

The Orbiter structure is made of aluminum skin/stringer, aluminum honeycomb, aluminum spar webs, aluminum ribs, graphite epoxy skin and honeycomb panels, inconel hinges, boron/epoxy truss tubes and titanium/boron thrust structure. The thermal protection system is made of reusable surface insulation (RSI) tiles over the upper and lower surfaces of the Orbiter structure, thermal blankets over the cargo doors and upper surface, and reinforced carbon-carbon (RCC) on the leading edge of the wings. The Orbiter structure was designed for 10 years and 100 operational flights with a safety factor of 4 (10-year Design Service Objective). The fleet leaders OV102 and OV103 have 26 flights each, OV104 has 20 flights, and OV105 has 15 flights. Plans are currently under consideration to continue flying the Space Shuttle until the year 2012, but many have quoted 2020. Because the Shuttle is nearly 20 years old, the issue of an aging structure and aging sub-systems must be addressed to safely operate the Shuttle into the next millennium.

The External Tank (ET) was not covered in the SIAT reviews but the external tank is made of welded aluminum-lithium (2195) sections and this material has lower fracture toughness than the previous material (2219). An issue is raised about the inspection and proof-test logic to screen for flaws or cracks at room temperature and operate at cryogenic temperatures.

## Assessment

### Orbiter Structure

Recent events that have occurred on the Orbiter Discovery (OV103), in preparation for the early December 1999 flight, are very disturbing. These problems point to poor workmanship and improper inspection verification on the Orbiter (i.e., stamping inspection documents without inspecting the vehicle or components). Stamping an inspection document without inspecting the vehicle is a clear violation of the condition of employment and is grounds for dismissal. The root causes of these workmanship and inspection problems are serious issues that need to be resolved. This discovery raises the question of where do priorities lie? Are there enough quality inspectors and is the schedule more important than quality and safety?

The large reduction in NASA Quality assurance Inspectors for each Shuttle is very disturbing. The corresponding reduction in the number of problems reported may also have a direct relationship to the reduced number of inspectors.

From the recent investigations on aging aircraft fleets (Industry Aging Aircraft Working Group and the Government sponsored research programs), some key considerations are to: (1) maintain accurate record keeping, (2) timely communication between data collectors (or data processors/evaluators) and decision makers, especially in small fleets, such as the Space Transportation System, (3) improved inspection methods for cracks and hidden corrosion, and (4) improved lifing methodologies for complex, built-up structures.

Use of fatigue-crack-growth thresholds in life calculations – The original Orbiter structure was designed with the Safe Life concept (a fatigue based life assessment) but early in the Shuttle development, the use of the Damage Tolerance (DT) concept was adopted. An early reference for this approach is the Space Shuttle Orbiter Fracture Control Plan<sup>16</sup> from Rockwell International. This approach assumes an inspectable flaw size (i.e., 0.05 inch crack at critical locations in the structure) to prevent failure of the structure due to crack propagation during fabrication, testing, handling, and the operational life of the vehicle. A static test was conducted on OV099, but no full-scale fatigue test was conducted. But many components or sub-components in the structure were subjected to extensive testing for fatigue life and static failure. Most of the Orbiter structure and components have fatigue lives that are well in excess of the 400 flights (design life).

(With a factor of 4 on life, the operational life is 100 flights.) There are a number of critical parts or components that just met the design life calculations from the Damage Tolerance (crack growth) approach. Fatigue-crack-growth thresholds from the early literature and those that were used in the original life analyses have now been shown to be too high for aluminum alloys and some titanium alloys, whereas high-strength steels show small differences. An assessment of using lower fatigue-crack growth thresholds and their impact on these critical parts or components needs to be reviewed to establish life and verify the inspection intervals.

Various structure and fracture critical components, such as those made of the aluminum alloy used in the construction of the Orbiters, were designed using damage-tolerance procedures. The crack-growth threshold ( $\Delta K_{th}$  or  $\Delta K_o$ ) values used for the aluminum alloy material are much higher than they should be based on new understandings of crack-growth behavior. The impact of using a lower threshold value (i.e., under zero to tension loading, either 0 or 0.8 ksi/in versus 3 ksi/in for aluminum alloys; 1.6 ksi/in versus 6 ksi/in for some titanium alloys; and 3 ksi/in versus 5 ksi/in for steels) on damage-tolerant life calculations for these fracture critical components need to be assessed. Specific hardware in question would be those components with a life close to the 100 missions (with a safety factor of 4). For example, the aluminum body flap attachment lug and the titanium thrust structure lugs.

Flight loads on the Shuttle Orbiter have been continually updated due to changes in structural weights and payloads. Assessments of the impact of these new loads are frequently made on the structure. These assessments should continue as responsibility for the Orbiter structure is transferred from the Government to the contractor.

An important question is whether inappropriately high fatigue-crack-growth thresholds were used to eliminate a substantial number of high frequency, small amplitude fatigue loading cycles in the operational loading history of the Shuttle. This has been a practice used by the aircraft industry to reduce the number of cycles in a load spectrum for testing and analysis, and would give optimistically high results if one were to use inappropriately high fatigue-crack-growth thresholds.

Crack growth retardation and acceleration models are not used in the assessment of life on the Orbiter structure. For most aircraft spectra (fighter and transports), crack growth is retarded due to overloads and the linear-accumulative-damage rules are conservative. But under some spectra, such as gust loading without these overloads, crack growth is accelerating and the linear cumulative damage rules are non-conservative. Retardation and acceleration model(s) should be used to assess the type of crack-growth history under the Orbiter spectra.

At the STS-103 Space Telescope Repair Mission Flight Readiness review on November 19, 1999, it was noted that the lower firtree lobes in the Shuttle main engine high-pressure fuel turbine had cracks. The stop tabs of the same turbine were also cracked. These cracks were reportedly caused by hydrogen assisted sustained load cracking. The cracks occurred with less than 4,000 seconds of Shuttle main engine run time. A review of the flight history of Columbia has shown that the main propulsion system has been exposed to hydrogen for over 1,000,000 seconds. This observation raises a concern about the potential for hydrogen embrittlement in the Orbiter main propulsion system's lines and valves.

## **Non-Destructive Evaluation Maintenance**

Every few years, the Orbiter is transported to Palmdale for major modifications and upgrades. During this time period, the Orbiter undergoes an intensive structural inspection. Visual and X-ray inspections are preformed over a large percentage of the structure. However, a large number of structural inspections are preformed with special inspection techniques, such as boroscope, eddy current, ultrasonic, and dye penetrant. The findings from these inspections are presented and discussed in documents<sup>17</sup>.

- During the past decade, the aircraft industry and the Government have developed approaches and methodologies to address an aging commercial aircraft fleet. The similarities between the aging commercial fleets and the small Shuttle fleet warrant new assessments based on these new understandings in the areas of non-destructive inspection and maintenance.

- 
- Corrosion of the honeycomb structure has been found under the thermal protection system in some locations using randomized intrusive searches. Non-intrusive inspection technique(s) for locating corrosion in hidden structures, such as under the tiles, need to be developed. A large number of advanced inspection techniques were investigated in the recent aging aircraft studies. Some of these methods, or modifications thereof, may be useful for inspecting the Orbiter with the tiles intact.

## Corrosion

In July 1993, the Orbiter Corrosion Control Review Board (CCRB) was established and chartered to advise the Space Shuttle Project Office and initiate resolutions for technical and operational activities involving corrosion. The reports on corrosion issues for the Orbiter<sup>18</sup> are very beneficial to attacking the corrosion problems and providing a lessons learned for future space vehicles.

Based on the Structural Inspection Report (OV104), corrosion is one of the key findings during inspection. Corrosion issues will increase with age due to the environments at the launch and landing site(s).

Hidden corrosion problems require a proactive inspection program with practical and reliable non-destructive evaluation techniques. The use of corrosion preventive compounds (CPC) is approved for certain areas that have experienced severe to moderate corrosion. Additional topics for review include:

- To date, much of the corrosion damage discovered has been largely unanticipated in the design of the Shuttle, and results of extending its operational life. Identifying hidden corrosion damage in built-up structure is difficult (no corrosion detection/inspection standard exists for quantifying such damage), and typically to find such damage it is necessary to disassemble the structural elements. Furthermore, about 10 percent of the structure is inaccessible, but this varies on each Orbiter. Given the uncertainty of inspection for such built-up or inaccessible areas, it appears logical to assess the risk of structural failure (from all mechanisms of failure) due to the presence of potential levels of corrosion damage. Such analyses would account for increased stress due to lost area or to the potential initiation of new unanticipated pits, which may be larger than, or equivalent to, the current 0.050-inch initial crack used in damage tolerant analyses. Sensitivity studies could help justify disassembly when the potential risk of structural failure (loss of fail safety) is high due to the presence of non-inspectable corrosion damage.
- The Corrosion Control Review Board should continue to explore the use of CPCs that are water displacing and contain corrosion inhibitors for their value to wick into joints that could trap water and lead to hidden corrosion.
- The 1995 and 1997 reviews of Space Shuttle Orbiter corrosion history by the Corrosion Control Review Board indicate that the corrosion prevention systems have been breaking down and inspection is now the primary strategy for identifying and controlling corrosion. The primary protection of the Orbiter is via a coating system that is based on chromate conversion coating and a chromated epoxy amine primer (referred to as Super Koropon), and this coating system has an expected life of about six (6) years. In selected areas, a polyurethane top coat is applied. The 1997 review discusses the importance of seeking alternate (replacement) coating systems that are more corrosion resistant and less likely to microcrack under operational flexure loading. This 1997 review also indicates that very little funding has been set aside address evaluation of any replacement coatings. Since the initial design life of the Orbiter was 10 years, it is not surprising that the corrosion protection systems are failing. To meet the currently expected 30-40 years of service, it will be necessary to direct additional effort into identifying better ways to control the level of corrosion before it becomes widespread. Increasing the corrosion resistant level of the coating system is one method of reducing the potential for widespread corrosion.

The 1995 Corrosion Control Review Board identified the use of the Orbiter corrosion database for tracking locations where corrosion has been identified as a result of past maintenance findings. It is obvious from the reviews that when serious corrosion problems are identified (either due to their impact to safety or recurring high maintenance cost) that action is being taken. However, there is a concern that as the Orbiter continues to age, more and more corrosion will occur, and it will be necessary to better track the occurrences and level

of damage. So the use of such a database is a positive step in ensuring proper corrosion control or structural maintenance action is taken before corrosion causes enough damage that it could impact the integrity of the Orbiter. To facilitate the use of such a valuable database, the suggestions made by the 1995 Corrosion Control Review Board should be implemented. Furthermore, the Orbiter database should make use of the Corrosion Prevention and Control Plan (CPCP) framework required by the Federal Aviation Administration by operators of commercial aircraft. This framework requires that the levels of corrosion damage be identified relative to the structural limits established by the OEM. Given the importance of the Orbiter fleet, the database should document all corrosion findings using photographs of the corrosion observed, and the subsequent repairs.

With corrosion issues increasing with age, the Corrosion Control Review Board should stay very active and aggressively attach the present and future corrosion problems. It is recommended that the Corrosion Control Review Board continue to report the findings in NASA or like publications.

## **Thermal Protection Systems**

The thermal protection system of the Space Shuttle Orbiter is unique among other atmospheric reentry vehicles in that it, along with other Orbiter sub-systems, is reusable. During a typical reentry heating cycle, the Orbiter is subjected to temperatures in excess of 2,300°F. The thermal protection system is composed of the reusable surface insulation tiles (upper and lower Orbiter surface), advanced flexible reusable surface insulation (AFRSI) thermal blankets (upper surface), and reinforced carbon-carbon (RCC) on the leading edge of the wings.

- The thermal protection system is very sensitive to process changes and quality control must be maintained to keep a functional system. A high level of inspection must be maintained to find imminent problems. The number of government mandatory inspection points (GMIP) should not be reduced any further. There are concerns that reduced manpower will erode previous very extensive inspections, and hence, safety of the thermal protection system.

## **External Tank**

The superlight-weight tank (SLWT) is made of 2195 aluminum-lithium alloy which has a lower fracture toughness than the 2219 aluminum alloy used in the light-weight tank (LWT). It would be expected that this material would have more welding induced cracks than the previous material. The external tank uses a room temperature proof to screen for flaws with the logic that the failure stress for a given flaw size at room temperature will fail at a lower stress than at the operating cryogenic temperature. For small cracks, the aluminum-lithium alloy does fail at a higher stress at cryogenic temperature (liquid oxygen and liquid hydrogen) than at room temperature (temperature during proof test). Thus, the proof test can screen for flaws or cracks, if they are small. However for larger cracks, the reverse is true. This means that the fracture-toughness ratio (FTR) can not be greater than 1.1 for the larger cracks. The SSP should determine the crack size that would maintain an FTR = 1.1 (for the parent material and the welds) and review that appropriate inspection procedures are in place to screen the Super Light-Weight Tank before and after proof. An additional concern is whether the Fracture-Toughness Ratio has been lowered from 1.1 to 1.0, and if so, a review of the rationale for lowering it.

The room temperature proof-test logic is satisfactory for small flaws or cracks and it is not recommended that this be changed. However, the pre- and post-proof test inspections must then be adequate to find the larger flaws or cracks. Non-Destructive Evaluation methods are often quoted with the smallest flaws or cracks that can be found, however, it is the largest flaw or crack that can be missed during an inspection that is of utmost importance. It is this largest flaw or crack that may not be screened by the room temperature proof test.

## Summary

The Shuttle vehicles have relative few flight cycles compared to most other aircraft; however, their age and the harsh environment in which they operate mandate stringent inspection and maintenance practices. Many aging aircraft practices and techniques are directly applicable to Shuttle. More accurate structural life prediction and inspection methods have been developed since the design and early maintenance of the Shuttle and should be pursued. Methods for identifying and controlling corrosion, an increasing problem for Shuttle, may also be available. Because no redundancy exists for much of the Orbiter structure and many mechanical components (e.g., landing gear), structural maintenance and inspection processes can significantly impact Shuttle safety and should be improved according to the recommendations listed above.



## Wiring

### Findings

1. The SIAT believes visual wiring inspection can not identify 100% of all wiring anomalies. The program will have to assume a certain percentage of wiring anomalies are present in each of the vehicles. Although functional tests are performed following vehicle close-out, these tests cannot detect all types of wiring defects (see Finding 18).
2. A major difference between Shuttle and aircraft wiring is the high touch labor level and the intensity of maintenance actions on and near Shuttle wiring. While Shuttle wiring was shown to be resistant to damage<sup>19</sup>, extensive damage was present and is attributed to vehicle processing and maintenance. This leads to a concern that adjacent systems may have also experienced damage.
3. Aging of Shuttle wire has occurred due to handling damage, environmental damage (heat, ultraviolet radiation, moisture, mechanical stresses, exposure to high pH fluids), chafing/vibration, exceeding wire bend radiuses, the large number of wire repairs, and electrical degradation from repeated testing. However, the extent and degree of damage that has occurred is not known.
4. The pedigree of the wiring is not well documented. It appears that a large amount of the wiring damage may have occurred many years earlier. During the life cycle of the Orbiters, there apparently have been variations in repair and inspection processes, changes to quality assurance practices, lack of quality surveillance inspections on wiring and other Shuttle hardware, differences between Palmdale and Kennedy Space Center processes, specification changes, and some degree of wire aging/degradation as a result of environmental exposure and repair actions.
5. Single point failure conditions exist in wiring which compromise redundancy in systems identified as critical. While it may not be possible to always separate all wiring it is important to identify areas where critical wiring is combined. Understanding wiring impact on redundancy would also aid in conducting risk assessments.
6. The current inspection process requires inspectors to examine wiring using flashlights, mirrors, and up to 10X magnification (*Figure 22*). This typically requires damage to be visible from the top of the wire bundle or in an area known to be susceptible to damage (*Figure 24*). There have been at least two instances where wire damage was inside a bundle and not obvious during external inspections.
7. The STS-93 wiring in-flight anomaly was never treated as an incident or mishap investigation, and no formal analysis was conducted to determine what processes broke down to result in the extensive wire damage found in all four vehicles.
8. Three arc tracking events have occurred on space transportation vehicles, two of them associated with the Space Shuttle. These events, although rare, indicate the Shuttle is susceptible to arc tracking and that current circuit breaker technology does not mitigate this risk. Further, as polyimide insulation ages, the frequency of arc tracking events typically increases.
9. The technicians that are working on the wiring are certified, yet some lack detailed/specific experience with wiring. Some of these technicians have extensive experience working on many Shuttle operations yet limited time inspecting and repairing wiring. In some cases, the technicians were given training just prior to the start of the recent wiring inspection and repair effort.
10. The SIAT is concerned that experience and expertise with polyimide insulated wiring within NASA and other agencies was not adequately identified or considered by the NASA and USA SSP wiring team members. The lack of understanding may have influenced the SSP personnel to limit their investigation of the wire incident to only a small subset of potential problems.

11. During the inspection of wiring, several connector issues were also apparent. Loose connector backshells and wire strain relief that can potentially chafe wiring were noted. Under certain conditions loose backshells can compromise electrical bonding between shielding and structure. Movement of the backshell can also cause chafing between the wiring and strain relief.
12. During cursory inspections several SIAT members noted foreign object debris and wire anomalies (*Figure 27*). While at the Palmdale Shuttle facility, metal shavings were noted in the mid-body of vehicle 102 (*Figure 25*). Shavings were noted on wire bundles and on the walking platforms. At Kennedy Space Center an apparent metal shaving was found embedded in a wire bundle (*Figure 28*). These occurrences are considered potential sources of foreign object debris and could damage surrounding wire insulation or provide an electrical shorting path.
13. In some applications a Hex head type screw will be used to replace the Phillips screw (*Figure 29*). The hexagonal head may also be a chafe source.
14. It is apparent that the current wire tray design contributed to STS-93 wiring failures. The use of a wire tray allows wiring to touch metal surfaces, which results in the wiring contacting screw heads and other sharp surfaces. The reuse of tray screws and an occurrence of burred screw heads have created an unexpected chaffing source (*Figure 27*).
15. Age assessment of selected wire samples is necessary to baseline the insulation condition. Further, single point failure potential conditions exist subject to maintenance error and require the utmost inspection attention. There has been no quantification of defects found, but the SIAT suspects that upon follow-up inspection, additional defects would be found.
16. Wire modifications and repairs have reduced the integrity of the overall wiring. Each repair adds an insulation shrink material that stiffens the wire and requires heat for application. The handling during modification and repair also stresses the wiring. Polyimide wiring is known to be notch sensitive. Small nicks or defects can be propagated down to the conductor when tensile loads are applied to the wire.
17. The SIAT is concerned that lessons learned from the wiring incident or mishap may not be applied to other sub-systems (such as hydraulics, electrical panels, recent modifications-glass cockpit, upgraded avionics, and other sub-systems).
18. Electrical integrity checks on Shuttle wiring consists of functional electrical checks and in some cases applying a 1500 VDC dielectric breakdown voltage between isolated wiring. In either case, this will only locate a severed connection or a shorted wire. A wire with an exposed conductor that is not in direct contact with another wire or metallic structure would most likely not be detected. Even at 1500 VDC, the dielectric breakdown test will be passed if the separation between the conductor and potential leakage path is more than several millimeters.

## Recommendations

1. The reliability of the wire visual inspection process should be quantified (success rate in locating wiring defects may be below 70% under ideal conditions).
2. Wiring on OV102 at Palmdale should be inspected for wiring damage in difficult-to-inspect regions. If any of the wires checked are determined to be especially vulnerable, they should be re-routed, protected, or replaced.
3. The need to examine wiring in areas that are protected or where damage may be induced by physical wiring inspection should be evaluated. Wiring should be continuously evaluated by conducting extensive electrical verifications on systems. When wiring damage is found in an area previously not examined, the remaining Orbiters should also be inspected.
4. Wire aging characteristics should be evaluated, including hydrolysis damage, loss of mechanical properties, insulation notch propagation, and electrical degradation. Testing should be performed by an independent laboratory.

- 
5. Wiring subjected to hypergolic contamination should be replaced since high pH fluids are known to degrade polyimide type wire insulation.
  6. The 76 CRIT 1 areas should be reviewed to determine the risk of failure and ability to separate systems when considering wiring, connectors, electrical panels, and other electrical nexus points. Each area that violates system redundancy should require a program waiver that outlines risk and an approach for eliminating the condition. The analysis should assume arc propagation can occur and compromise the integrity of all affected circuits. Another concern is that over 20% of this wiring can not be inspected due to limited access; these violation areas should as a minimum, be inspected during heavy maintenance and ideally be corrected.
  7. Current wire inspection and repair techniques should be evaluated to ensure that wire integrity is maintained over the life of the Shuttle vehicles. Several new inspection techniques are available that use optical, infrared, or electrical properties to locate insulation and conductor damage, and should be explored for use on the Shuttle.
  8. Failure analysis and incident investigation should identify root cause and not be artificially limited to a sub-set of possible causes.
  9. A database that continually evaluates wiring system redundancy for the current design, modifications, repairs, and upgrades should be maintained. System safety should evaluate the overall risk created by wiring failures.
  10. All CRIT 2 circuits should be reviewed to determine to what extent redundancy has been compromised in wiring, connectors, electrical panels and other electrical nexus points. The primary concern is that single point failure sources may exist in the original design or have been created by system upgrades or modifications.
  11. Arc track susceptibility of aged wiring and circuit protection devices that are sensitive to arcing should be evaluated.
  12. The current quality assurance program should be augmented with additional experienced NASA personnel.
  13. Technician/inspector certification should be conducted by specially trained instructors, with the appropriate domain expertise.
  14. NASA and USA quality inspection and NASA engineers should review all CRIT 1 system repairs.
  15. NASA engineering should specifically participate in industry and government technology development groups related to wiring. The SAE AE-8 committees (specifically A and D) are excellent forums for identifying wiring issues.<sup>20</sup>
  16. Due to time constraints, the SIAT only examined Orbiter wiring; many other systems associated with the Shuttle also have critical wiring. The findings and recommendations in this report are applicable to all Shuttle systems, but unique conditions that may require additional actions.
  17. The Shuttle program should form a standing wiring team that can monitor wire integrity and take program wide corrective actions. The team should include technicians, inspectors, and engineering with both contractor and government members. The chair of the team should have direct accountability for the integrity of the Shuttle wiring. The techniques that can detect an exposed conductor that has not yet developed into an electrical short should be evaluated.
  18. Loose connector backshells and wire strain relief that can potentially chafe wiring are unacceptable conditions and should be eliminated by periodic inspection and connector redesign.
  19. A formal Aging and Surveillance Program should be instituted.
  20. The long term use of primarily polyimide wiring should be minimized, and wire insulation constructions that have improved properties should be evaluated and compared to the current wire insulation used on the Shuttle program. Alternate wire constructions should be considered for modifications/repairs/upgrades. There are several aerospace wire insulation constructions that can provide more balanced properties.
  21. Where redundancy is used to mitigate risk, it should be fully and carefully implemented and verified. If it cannot be fully implemented due to design constraints, other methods of risk mitigation must be utilized.
-

## Introduction

The SIAT was requested to review maintenance practices, identify systemic issues, suggest techniques or approaches that can increase system safety, and recommended actions prior to next flight. The SIAT participated in most meetings related to wiring since this was a high interest item.

The SIAT was briefed on an in-flight anomaly wiring failure that occurred during the STS-93 mission of OV102 Columbia. Five seconds after the STS-93 launch, a primary and back-up main engine controller on separate engines dropped offline. Controllers were automatically dropped off line when a power fluctuation was detected. This left single engine controllers on two of the three engines (each main Shuttle engine has double redundant controllers). The mission continued uneventfully and after the mission, inspection revealed a single 14 ga. polyimide wire had arced to a burred screw head (*Figure 17* and *Figure 18*). The wire was located in the aft left-hand mid-body bay #11 lower wire tray. A single three amp circuit breaker had tripped, with no electrical damage to adjacent wiring. The wire provided 115 VAC power to each of the controllers that were dropped off line.

Technicians noted a 10 ohm short between the wire electrical ground through the structure of the vehicle. Inspection of the wires in the adjacent area revealed insulation and conductor damage at the short location (*Figure 18*). An expanded inspection of all mid-body wires revealed varying degrees and types of wire insulation damage. All four vehicles exhibited extensive and varying degrees of wire insulation damage from exposed conductors to minor abrasion (*Figure 19*, *Figure 20*, and *Figure 21*). The SIAT was briefed on the Shuttle program analysis of the in-flight anomaly, the results of inspection and repair of wiring on all vehicles, and corrective actions taken to mitigate future wiring failures. In the course of the SIAT's fact-finding process, we reviewed maintenance practices and representative vehicles at the Kennedy Space Center Shuttle processing facility and the Palmdale Shuttle depot facility.



Figure 17 -- Shorted Wire in OV102: Arc Damage & Mechanical Damage

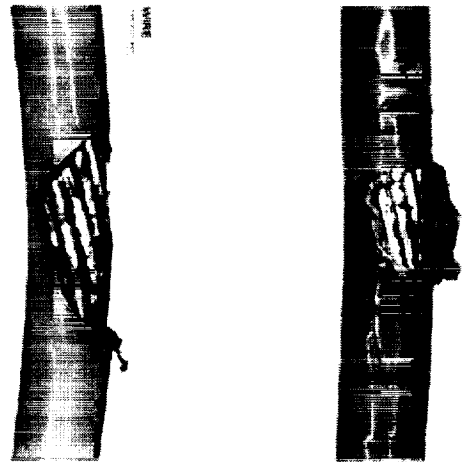


Figure 18 -- Carbonized Insulation Due to Arc Damage

## Assessment

### STS-93 Wiring In-Flight Anomaly

First, the SIAT considered the in-flight anomaly to be an incident or mishap, given the potential for loss on an engine following the event since two of the three engines had single controllers, compromising system redundancy. The potential loss of a main engine during launch was considered to be a serious enough condition to warrant a full mishap investigation.

The following is an assessment of the wire incident or mishap based on presentations given by NASA and on NASA laboratory data. The material transfer and welding present provide evidence of arcing; gouges in the conductor were also noted. Surface analysis revealed oxides in the wire strand gouge sites that suggest the damage might have occurred several years earlier. The wiring in the mid-body payload bay is normally covered and records did not indicate the cover had been removed since the last Orbiter Maintenance Down Period (OMDP) that occurred four years earlier at the Palmdale depot facility. Secondary damage caused by the arcing has destroyed most of the insulation and wire damage that was present before the arcing began at the primary failure site. Circumstantial evidence surrounding the failure suggests the wire may have initially been damaged by an impact and subsequent chafing/vibration may have led to the electrical failure. There was no evidence of arc propagation into adjacent wiring.

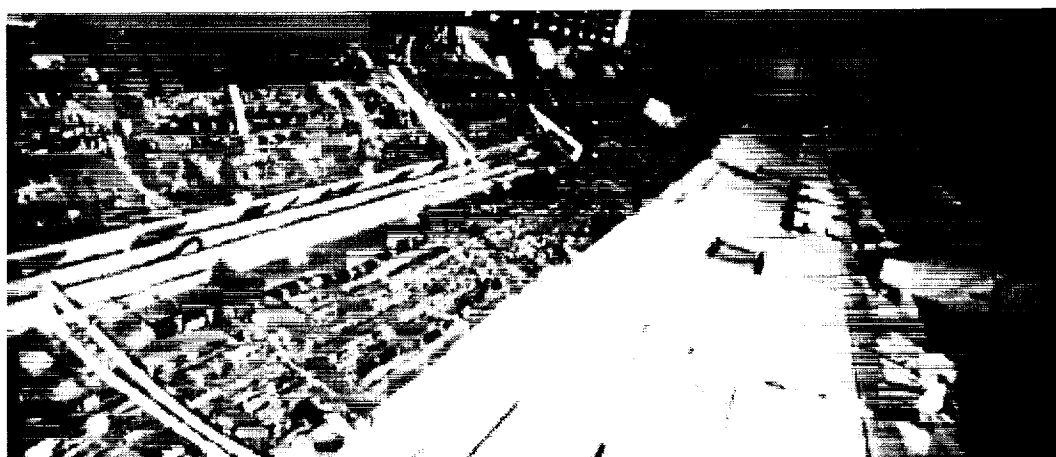


Figure 19 -- Red Tag Anomalies in OV103 Left Mid-Body

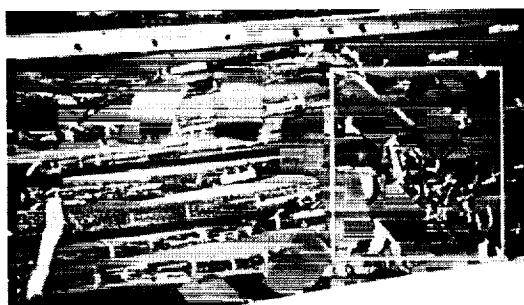


Figure 20 -- Close-up OV103 Mid-Body: Compromised Redundancies, Possible Chafing



Figure 21 -- OV103 Mid-Body: Intersecting Wire Bundles

The failure does not appear to be related to properties unique to polyimide insulation, any thin walled insulation would be susceptible to this type of failure. When an arc event occurs, polyimide can carbonize and propagate damage into adjacent wiring. Outer edges of the mishap polyimide wire appeared to be carbonized, this would have created a low resistance path between the conductor and another metallic surface. During the arc event a three ampere circuit breaker "popped", suggesting there was a hard short. The presence of a hard short is also supported by evidence that the wire and screw head were welded together and separated after the arc had cooled. This is supported by the presence of ductile dimples, characteristic of overload, in the weld area. Polyimide failures that propagate or arc track tend to be resistive or "soft shorts". This type of fault would appear as an intermittent load. Insulation damage was noted under and near the screw head. Normal inspection procedures could have missed this type of damage.

The screw head associated with the arced wire exhibited a raised burr, which may have been formed when the screw was removed and then replaced (*Figure 17*). Most of the screw head appeared to be coated with an insulating material (Koropon). The coating may have protected the exposed wire in previous launches. At 115 volts, the exposed wire would have to touch a bare part of the screw head to arc. Vibration during the launch sequence was apparently sufficient to allow contact between the exposed conductor and an exposed metal area on the screw head.

A second area of insulation damage was noted on the mishap wire several inches from the failure site. This site was also associated with a screw head, having a raised burr on the counterclockwise side of the Philips screwdriver slots. The damage site was on the underside of the wire and exposed the conductor. There was no arcing evidence, however, gouges were noted in the conductor strands. The layered polyimide insulation appeared to have been scuffed off by contact with the screw head. The damage is consistent with an impact (e.g., possibly being stepped on while the wire in the wire tray was uncovered).

Other examples of insulation damage were reviewed. The source of damage was most likely a one time impact event, however, chafing from vibration between another structure and the wiring could not be completely ruled out. Analysis was inconclusive due to the lack of baseline data on known exhibits with vibration and impact damage.

### **Wiring In-Flight Anomaly and Corrective Actions**

The NASA Shuttle program determined the root cause of the wiring in-flight anomaly was workmanship and there was no evidence of aging/degradation of the wiring. It was not considered to be a mishap, since the failed wire was a CRIT 1R/3 system, and the incident itself did not cause injuries or exceed the dollar threshold to initiate a mishap investigation.

Corrective actions taken by the program included detailed inspection of all mid-body wiring and selected inspection of additional wiring, repair of wiring damage, redefining and standardization of wire inspection criteria to allow for less damage, and additional protection was added to selected critical wiring.

The return of the Shuttle to flight status, with respect to wiring, was based on repair of wire damage, wiring failure mitigation by overall Orbiter design, and maximum feasible separation of redundant systems.

### **Maintenance Requirements**

Each Shuttle vehicle contains over 200 miles of wiring throughout the vehicle. As with modern aircraft, Shuttle wiring is a critical system since multiple failures can lead to loss of a vehicle. The primary wiring used in the Shuttle is a nickel-plated copper conductor with 6 mil thick polyimide/FEP insulation (similar to MIL-W-81381, trade name "Kapton", a wire construction extensively used in aviation from the early 1970's to mid 1990's). While this insulation has performed well in many applications, there are known issues related to arc track propagation (carbonization of polyimide and rapid collateral damage to adjacent wiring), mechanical degradation when exposed to certain environments (ultra-violet radiation, high pH materials (>10), sustained long term exposure at elevated temperatures to moisture while under mechanical stress), and insulation cracking when the insulation is nicked and placed under tensile stresses. Polyimide wire insulation performs best in straight runs with minimal bending and flexing. Examination of the Shuttle mid-body would seem to be

the ideal application for this type of wiring (*Figure 19*). The extensive wiring damage found on each vehicle (see Table 4 – Summary: Reported Wiring Anomalies on 3 Orbiters (NASA, USA)) appears to be related to the high and continuous exposure to personnel performing maintenance procedures on various Shuttle systems.

Inspectors have been encouraged not to conduct intrusive inspections to minimize induced wire damage. The most intense inspection has been conducted in the mid-body bays. A summary of the areas inspected in the mid-body and aft areas is shown graphically in . An examination of the Problem Resolution and Corrective Action system data prior to recent inspections shows the mid-body area to be the fourth highest area with wire damage (*Figure 30*). The data as of November 18, 1999 shows that since the recent inspections in late August 1999, there have been 485 PRs written related to wiring in the mid-body area (see Table 4). Examples of the type of wire damage being found are shown in *Figure 23* and *Figure 24*. Note that in *Figure 23* the conductor is exposed and has broken strands.

**Table 4 -- Summary: Reported Wiring Anomalies on 3 Orbiters (NASA, USA)**

<u>Area</u>	<u>Total PRs</u>	<u>Kapton Damage</u>	<u>Exposed Conductor</u>	<u>Other</u>
<b>OV103</b>				
Forward	34	25	4	6
Mid-Body	160	84	26	52
Aft	164	87	28	52
Total	358	196	58	110
<b>OV105</b>				
Forward	25	16	1	4
Mid-Body	169	93	64	34
Aft	74	24	2	31
Total	268	133	67	69
<b>OV104</b>				
Forward	13	0	0	0
Mid-Body	156	137	64	17
Aft	94	0	18	0
Total	263	137	82	17

## Design Issues

According to an early 1990's NASA study, the redundancy in 318 CRIT 1 circuits were compromised by placing the redundant circuits in the same wire bundle or clamp. There were 129 CRIT 1/1 areas identified that violate system separation requirements. NASA Standard 8080 requires that critical circuits be physically separated. As an example, six separate areas exist that, if compromised electrically, would result in the loss of all main engine controllers. A review of the data indicates only violations that could be eliminated required a waiver. At the time of this report, a review of CRIT 2 systems with respect to comprising redundancy was pending.

It is apparent the current wire tray design contributed to STS-93 wiring failures. The use of a wire tray allows wiring to touch metal surfaces, which has resulted in the wiring contacting screw heads and other sharp surfaces. A past and possibly current maintenance practice has changed tray design assumptions. The reuse of tray screws and an occurrence of burred screw heads have created an unexpected chaffing source (*Figure 28*). There was also considerable configuration variability between vehicles. In some cases additional chafe protection was added or screw heads were covered with a protective coating. The wire bundles were permitted to move in clamps and the trays. Typically, critical circuits must be kept physically separated from all surfaces and other wiring.



Figure 22 -- Wire Defect Inspection Process

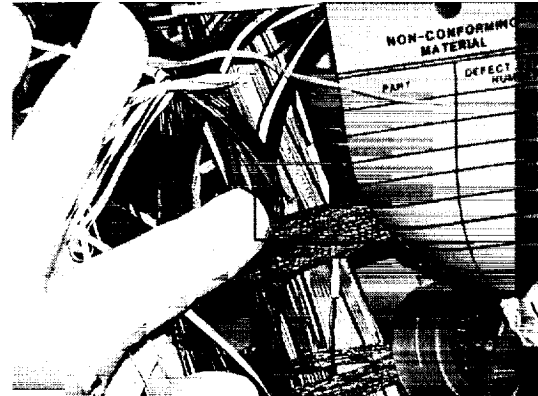


Figure 23 -- OV103 Mid-Body: Strand Damage

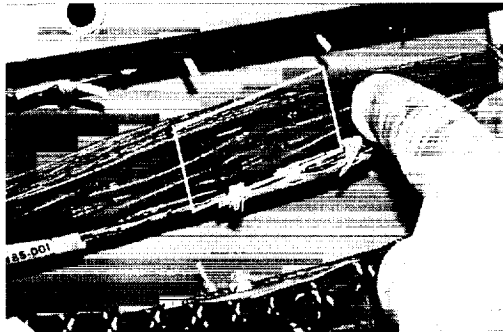


Figure 24 -- Surface Damage Inside Bundle

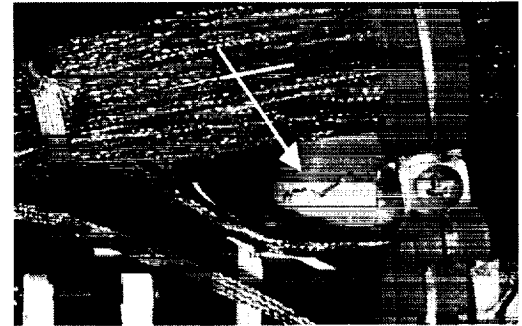


Figure 25 -- OV102: FOD, Metal Shaving

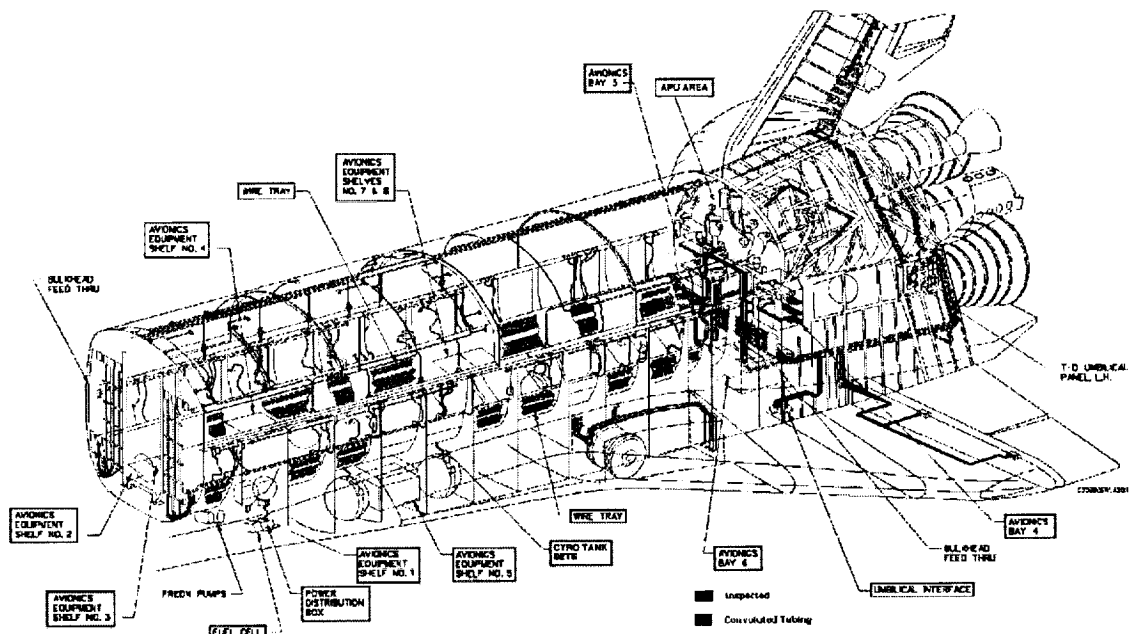


Figure 26 -- Inspected Areas



# SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT



Figure 27 -- Potential Chafe in Mid-Body

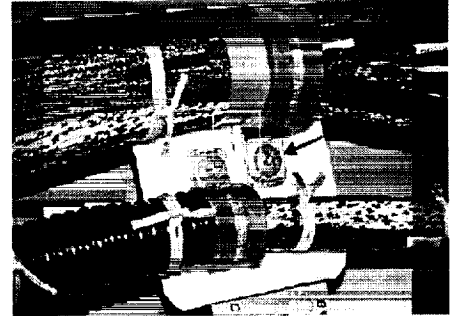


Figure 28 -- Metal Shaving (FOD), Burred Screw, Convolved Tubing

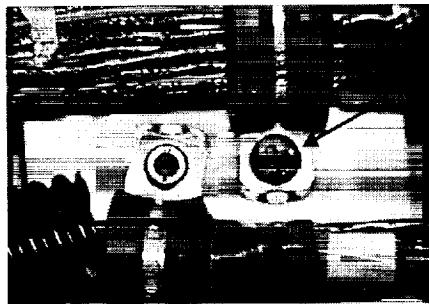


Figure 29 -- Burred Screw, Hex Head Screw

## PRACA SUMMARY (FWD/MID/AFT)

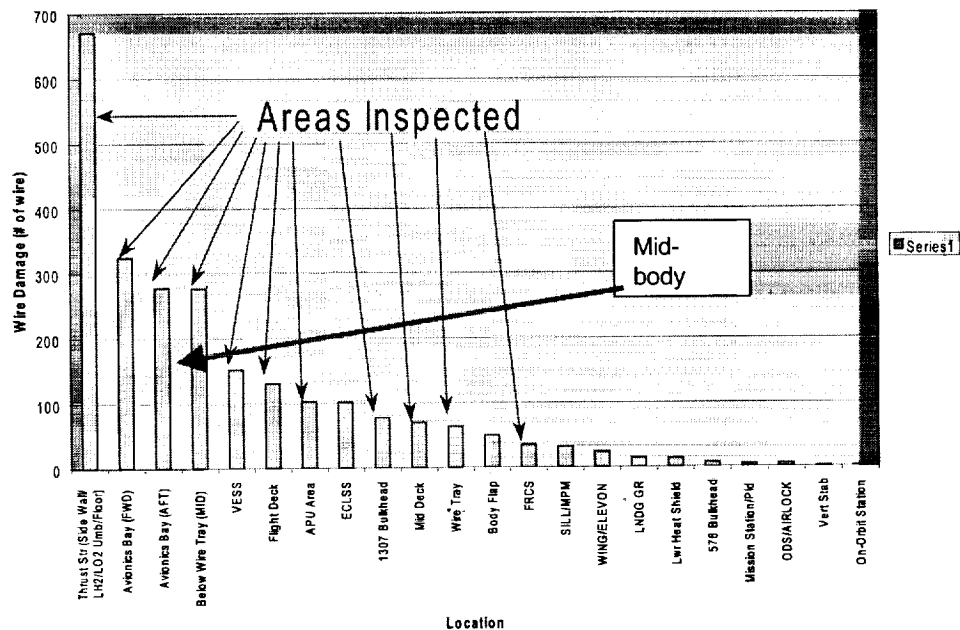


Figure 30 -- Summary of Wire Damage, Prior to Recent Inspections

## Arc Tracking

Damage to wiring or insulation and aging of insulation are a concern to the Shuttle fleet. Several incidents have been recorded<sup>21, 22, 23</sup> over the life of the program.

As the Shuttle fleet continues to age, additional problems are to be expected. Given the life expectancy of the Orbiters, it is essential to plan for maintenance related to aging, not solely for upgrades. As early as 1991, NASA documents reported that arc-tracking was a significant risk on the Shuttle, as identified in the following statement from the 1<sup>st</sup> NASA Workshop on Wiring for Space Applications, held at Lewis [Glenn] Research Center in July 1991: "Arc propagation poses a significant and credible threat to mission safety and success in aerospace vehicles [Shuttle]."<sup>24</sup> This workshop was attended by members of the Space Shuttle community including Johnson Space Center and was co-sponsored by NASA Headquarters, Code Q.

Arc tracking susceptibility has not been eliminated, as this is an inherent property of polyimide insulation. Laboratory tests have shown that current circuit breaker technology does not sense arc track events. Intermittent arcing is seen as a varying load by thermal circuit breakers and current spikes can exceed over 1000% of a circuit breaker's rating without tripping the device. Arc track events have occurred with one and three amp circuit breakers; many of the Orbiter circuits are protected by three amp breakers. Circuit breakers can also fail and not trip during an electrical short.

**Table 5 -- Space Missions with Electrical Wiring System Failures**  
(3<sup>rd</sup>. NASA Workshop on Wiring for Space Applications, July 1995)<sup>25</sup>

<u>Mission</u>	<u>Cause</u>	<u>Result</u>
Gemini 8	Electrical wiring short	Shortened mission-near loss of crew
Apollo 204	Damaged insulation, electrical spark, 100% ) O <sub>2</sub>	Fire, three astronauts lost
Apollo 13	Damaged insulation, short circuit/flawed design	Oxygen tank explosion, incomplete mission
STS-6	Abrasion of insulation/arc tracking	Wire insulation pyrolysis, 6 conductors melted
STS-28	Damaged insulation, arc tracking	Teleprinter cable insulation pyrolysis
Magellan	Wrong connection, wiring short	Wiring insulation pyrolysis
Spacelab	Damaged insulation, arc tracking	Wiring insulation pyrolysis during maintenance
Delta 178 / GOES-G	Mechanical or electromechanical insulation damage	Loss of vehicle
ESA-Olympus	Electrical wiring short	Loss of solar array

## Summary

Wiring on the Shuttle orbiters must withstand considerably different environments than the wiring on commercial and military aircraft. In particular, the maintenance environment is intrusive and causes significant amounts of collateral damage. The Shuttle wiring, however, is also susceptible to degradation known to occur in similar wiring applications, including insulation aging, and may experience similar failure modes, such as arc tracking. Hence, Shuttle processing of wiring must incorporate lessons learned from industry and military experience as well as adhere to unique, stringent requirements for inspection and maintenance. The SIAT is encouraged by the current attention given to wiring by the Shuttle Program. As the number of findings and recommendations attest, though, there are still considerable improvements to be made. Of greatest concern is the lack of redundancy in a number of CRIT 1 circuits, some of which are not accessible to inspection. The SIAT recommends that all improvements mentioned above be seriously evaluated and incorporated wherever possible.

---

## Section 5 - Recommendations

---

### Category 1: Immediate

#### Prior to Return to Flight

1. The reliability of the wire visual inspection process should be quantified (success rate in locating wiring defects may be below 70% under ideal conditions).
  2. Wiring on OV102 at Palmdale should be inspected for wiring damage in difficult-to-inspect regions. If any of the wires checked are determined to be especially vulnerable, they should be re-routed, protected, or replaced.
  3. The 76 CRIT 1 areas should be reviewed to determine the risk of failure and ability to separate systems when considering wiring, connectors, electrical panels, and other electrical nexus points. Each area that violates system redundancy should require a program waiver that outlines risk and an approach for eliminating the condition. The analysis should assume arc propagation can occur and compromise the integrity of all affected circuits. Another concern is that over 20% of this wiring can not be inspected due to limited access; these violation areas should as a minimum, be inspected during heavy maintenance and ideally be corrected.
  4. The SSP should review all waivers or deferred maintenance to verify that no compromise to safety or mission assurance has occurred.
- 

### Category 2: Short term

#### Prior to making more than four more flights

1. NASA should expand existing data exchange and teaming efforts with other governmental agencies especially concerning age effects.
  2. A formal Aging and Surveillance Program should be instituted.
  3. NASA and USA quality inspection and NASA engineers should review all CRIT 1 system repairs.
  4. The failure of all CRIT 1 units should be fully investigated and corrected without waivers.
  5. All testing of units must be minimized and documented as part of their total useful life. Similarly, maintenance operations must be fully documented.
  6. The SIAT recommends comprehensive re-examination of maintenance and repair actions for adequate verification requirements (e.g., visual, proof test, or green run).
-

- 
7. Human error management and development of safety metrics, e.g., Kennedy Space Center Shuttle Processing Human Factors team, should be supported aggressively and implemented program-wide.
  8. Communications between the rank and file work force, supervisors, engineers and management should be improved.
  9. NASA should expand on the Human Factors research initially accomplished by the SIAT and the Air Force Safety Center. This work should be accomplished through a cooperative effort including both NASA and AFSC. The data should be controlled to protect the privacy of those taking the questionnaires and participating in interviews. Since major failures are infrequent occurrences, NASA needs to include escapes and diving catches (see **Appendix 3**) in their human factors assessments.
  10. Maintenance practices should be reviewed to identify and correct those that may lead to collateral damage.
  11. Shuttle actuator soft goods should be adequately wetted to prevent downtime seepage.
  12. Tank time and cycle data must be carefully logged to ensure safe life criteria are not exceeded.
  13. Critical operations, especially those involving Self-Contained Atmospheric Protective Ensembles, must be staffed with technicians specifically experienced and properly trained with the operations.
  14. Fleet Leader testing must be carefully scrutinized to ensure adequate simulation of operating conditions, applicability to multiple sub-systems, and complete documentation of results.
  15. Vendor supplied training should be evaluated for all critical flight hardware.
  16. The true mission impact of a second main engine pin failure (internal engine foreign object debris) during flight, similar to that which took place last July, should be determined.
  17. The SSP should consider more frequent lot sample hot fire testing of the Solid Rocket Booster motor segments at full-scale size to improve reliability and safety and verify continued grain quality.
  18. An independent review process, utilizing NASA and external domain experts, should be institutionalized.
  19. NASA, USA, and the SSP element contractors should develop a Risk Management Plan and guidance for communicating risk as an integrated effort. This would flow SSP expectations for risk management down to working level engineers and technicians, and provide insight and references to activities conducted to manage risk.
  20. Risk assessment matrix and Failure Modes and Effects Analysis should be updated based on flight failure experience, aging and maintenance history, and new information (e.g., wiring, hydraulics, etc.).
  21. The SSP should revise the risk matrix for probable and infrequent likelihood for critical 1R\*\* and 1R\* severity to require a greater level of checkout and validation.
  22. NASA Safety and Mission Assurance surveillance should be restored to the Shuttle Program as soon as possible.
  23. The Safety & Mission Assurance role should include: mandatory participation on Prevention/Resolution Teams and in problem categorization, investigation of escapes and diving catches (see **Appendix 3**), and dissemination of lessons learned.
  24. The SIAT believes that software systems (flight, ground, and test) deserve a thorough follow-on evaluation.
  25. Due to time constraints, the SIAT only examined Orbiter wiring; many other systems associated with the Shuttle also have critical wiring. The findings and recommendations in this report are applicable to all Shuttle systems, but unique conditions that may require additional actions.
  26. During the inspection of wiring, several connector issues were also apparent. Loose connector backshells and wire strain relief that can potentially chafe wiring were noted. Under certain conditions loose backshells can compromise electrical bonding between shielding and structure. Movement of the backshell can also cause chafing between the wiring and strain relief. In either case, these are unacceptable conditions and should be eliminated by periodic inspection and connector design.

Clearly, these trends would have to be researched for their relevance to NASA organizations. Nevertheless, these indicators are consistent with many of the emergent issues of the SIAT human factors observations and interviews.

## **Challenges in Maintenance Human Factors**

The contributing causes of human error in maintenance operations are not well understood. Because errors may remain latent over long periods of time and operational use, error event chains and their consequences are often difficult to trace and identify. In addition, human errors typically stem from multiple, interrelated sources; some are relatively easy to assess, such as workplace conditions or adequacy of resources; others are more indirect in their effect, such as organizational culture and communication barriers. Consequently, the process of managing error may involve multiple and diverse interventions with no single magic pill to cure the problems.

Maintenance human factors research has not had a long history. Although recent technology advances are found in many areas of maintenance operations, rarely have these innovations been accompanied by corresponding human factors development. The Federal Aviation Administration's Human Factors in Aviation Maintenance and Inspection program has been a pioneer in this area, but even this effort has a limited history. Thus, the primary technology challenge is the lack of an established research foundation of results, methods and metrics from which to grow. Technology transfer from other aerospace domains holds potential, but requires substantial adaptation for maintenance operations<sup>27</sup>.

Challenges in maintenance human factors also arise from the current operational and economic environment. Current conditions create significant changes and instability in maintenance organizations, from which emerge human factors issues. Roles and responsibilities of the workforce, regulations, company policies, and training needs are often changed. Cutbacks in resources and downsizing may result in an increased dependence on a contract labor force, and the associated problems of standardization and accountability. While process improvements and new technologies simultaneously streamline operations, there is often an associated process loss in terms of communication and training required.

In spite of these challenges, increasing numbers of innovative initiatives are being developed, implemented, and accepted for the purpose of safeguarding against human factors problems and maintenance error. Conscientious efforts have been made in re-inventing the "team" concept for maintenance operations and in tailoring human factors programs to fit their needs. However, there remains a dual challenge: 1) to develop human factors interventions which are directly supported by reliable human error data, and 2) to integrate human factors concepts into the procedures and practices of everyday technical tasks. Some of the major advances in maintenance human factors in the aviation industry are discussed below.

## **Human Error Management**

As the result of growing industry, government and research focus on maintenance error reduction, new investigation, analysis, and intervention strategies are becoming available to maintenance organizations.

The challenge, therefore, is to build an error management program that is properly tailored for the environment in which it is to function. Appropriate attention must be given to establishing an error threshold in order to define an error management program and to determine what resources and tools are required to support it. A low threshold error management program focusing on frequently occurring or common errors would require additional resources to conduct investigations and a greater capacity analysis tool to track error data. On the other hand, a program with the high error threshold of only investigating major events may require few resources, but would not collect sufficient information to identify trends before they lead to a significant error. A typical approach of maintenance organizations, which have successfully established program is to initially set a high error threshold and, as resources are developed and the process of investigating and analyzing errors becomes more efficient, the error threshold is able to be set at a lower level.

The error investigation process selected is of significant importance to the overall success of the error management program simply because it reveals the problem area. The means to collect the information surrounding an error may be based on a standardized form, on a computer database, or a combination of the

two. The investigation may be conducted by self-reporting, by a single investigator, or by a committee. A great deal of research has been undertaken by airlines, regulatory agencies, and academia to evaluate existing investigative approaches and to develop new ones<sup>28</sup>.

### ***Roundtable Meetings***

One of the various means of establishing an error management program is through Roundtable Meetings. To describe one implementation, the Federal Aviation Administration, IMAW, and US Airways' Management mutually agreed to develop a forum to address human factor-related errors that occur in the work place. All parties involved in the error participate in the meetings and issues for inclusion in Roundtable Meetings may be submitted by the Federal Aviation Administration, US Airways' Management, or the International Association of Machinists and Aerospace Workers. Unanimous consensus of all three parties is required before the meeting is held and an "Initial Error Notification" form is utilized for the initial advisement of an error. Since this program does not apply to infractions of regulations involving deliberate misconduct, serious deviations from required conduct, etc., meetings are based on the open and honest communication among management, labor and the Federal Aviation Administration. Error discussions are to be conducted in a problem-solving, non-accusatory, non-punitive manner. The roundtable committee, upon hearing the testimony, assigns action items and takes corrective action based upon its internal committee discussions. US Airways' Management and the IMAW MRM Committee representative jointly track the implementation of recommended actions.

### ***Maintenance Error Decision Aid (MEDA)***

The Maintenance Error Decision Aid (MEDA) process was developed as an aid to investigating the causes of maintenance and inspection errors. Boeing, working with three of its customers, British Airways, Continental Airlines, and United Airlines, developed and tested the MEDA process from 1992 through 1995. Since 1996, Boeing has provided MEDA implementation support to over 120 aircraft maintenance and engineering organizations worldwide.

The MEDA philosophy is:

- Mechanics/engineers/inspectors do not make errors on purpose
- Errors are due to a series of related, contributing factors in the mechanic/engineer/inspector's work area
- Most of these contributing factors are under the control of management and can, therefore, be improved to prevent future, similar errors.

Contributing to maintenance errors are a wide range of factors including 1) Information, 2) Equipment/tools, 3) Aircraft design/configuration/parts, 4) Job/task, 5) Technical knowledge/skills, 6) Individual factors, 7) Environment/facilities, 8) Organizational factors, 9) Leadership/supervision, 10) Communication. Existing data suggest that on average there are three to four contributing factors per maintenance error.

Experts estimate that between 70 per cent and 90 per cent of the contributing factors to maintenance/inspection errors are under the control of management and can, therefore, be improved to reduce the probability of future, similar errors. For example, poorly written manuals can be redesigned, poor lighting can be corrected, and calibrated equipment can be purchased. Only 10 to 30 per cent of the errors are due strictly to individual factors that are harder to improve.

Although MEDA has been widely accepted in the aviation industry, the tool itself is not so important as the support for human factors investigations in the first place. For instance, Northwest Airlines has used Boeing's MEDA, Aurora's Mishap Management System, and now uses an internally developed investigative system to conduct human error investigations. A culture must be set up where technicians feel a responsibility to participate in the learning culture, and management must be willing to take action on the items uncovered. Knowing where the disciplinary line is drawn and having a just disciplinary process was necessary to gain union support for the investigative process. Specific to the investigations themselves, Northwest Airlines now uses the rules of causation developed under research for the Federal Aviation Administration, and has set up specific investigative classes to ensure statistical validity in the

data collected. The objective of the Northwest program is to have a measurable effect on safety events and dispatch reliability--with the starting point being a 50% reduction in installation errors in the hangar operations.

#### Close Call Reporting

In addition to incident or mishap databases such as MEDA, other databases kept within the company may be structured in a variety of ways, and may be proactive as well as reactive measures. Industry-wide databases which have the advantage of detecting system-wide problems are maintained by manufacturers, the Federal Aviation Administration, and NASA Aviation Safety Reporting System (ASRS).

The Aviation Safety Reporting System (ASRS) was established in 1976 under an agreement between the Federal Aviation Administration and NASA. It is a unique program because it is a voluntary, confidential reporting system, which offers limited immunity to respondents. This incident reporting system invites pilots, air traffic controllers, flight attendants, maintenance personnel, and others to voluntarily report to NASA any actual or potential hazard to safe aviation operations. NASA administers the program, assures confidentiality, sets policies in consultation with the Federal Aviation Administration and the aviation industry, and receives the reports submitted to the program. Since April 1997, the ASRS has made a customized "maintenance version" available.

The ASRS collects and responds to voluntarily submitted incident reports to lessen the likelihood of aviation accidents. ASRS data are used to:

- Identify aviation system deficiencies for correction by appropriate authorities;
- Support aviation system policy, planning, and improvements;
- Strengthen the foundation of aviation human factors safety research.

Reports sent to the ASRS are held in strict confidence by NASA and thoroughly de-identified. More than 400,000 reports have been submitted since the program's beginning without a single reporter's identity being revealed.

## **Maintenance Best Practices**

### ***Human Factors Training***

A Maintenance Human Factors Program often includes a training element, which can encompass awareness training, skills training and human factors training focusing on specific areas that need improvement. An organization often begins their human factors program with a human factors awareness course for all of their maintenance and engineering personnel. This awareness course should familiarize participants with basic human factors principles and how these principles can influence their job performance. In addition, training is a vital communication vehicle for the Human Factors program in general. It is designed to facilitate the process of open communication between the workforce and all levels of management.

The goals and objectives of Human Factors (or Maintenance Resource Management--MRM) training should be consistent with the overall Maintenance Human Factors program in which it is an element. In some cases, Human Factors initiatives may be effectively linked. For example, data from one's error management system may help prioritize safety issues to be incorporated into the Human Factors training curriculum. Identifying the needs and constraints of the user group helps to focus training on known problem areas within the organization. It helps to tailor training content to specific workforce attributes (e.g., experience level, training requirements, skill mix) as well as to specific problems. For example, an increase in maintenance errors tied to incorrect or incomplete communication across shifts might suggest training on how to perform shift turnover procedures. The performance indicators underlying the error committed may also serve as safety metrics for gauging training effectiveness and process improvement over time.

Many U.S. and International airlines have implemented Maintenance Resource Management training as part of their corporate Safety programs or Training departments. Although programs vary according to their organizational philosophies, needs and resources, the industry has progressed rapidly due to the



free exchange of information and lessons learned in the aviation maintenance community. The current evolution of MRM is leading to "action-based" interventions, which are characterized by a commitment to long term behavioral changes that can be incorporated into daily practices. The emergence of MRM is becoming seen as more than mere "awareness training," or team-building exercises for mechanics; rather, it is the conscious process of increasing trust among maintainers, their managers, and their regulators.

For example, Northwest Airlines implemented a 4-hour human factors course that raised awareness to human factors concerns among the workforce. However, it is now clear from the Northwest experience that awareness training cannot stand alone as a human factors intervention. Without specific behaviors for manager and employees to engage in, awareness training will provide little demonstrated reductions in safety events. Northwest is currently designing its phase two human factors training program focused more specifically on affirmative duties and roles of both technicians and managers in the overall human error management effort.

### **Other Human Factors Interventions**

In addition to Human Factors training (awareness and action-based training), there are other ways to support the workforce (sometimes called ergonomic interventions). Human Factors/Ergonomics professionals look at a problem from two viewpoints in order to determine whether to *fit the job to the person and/or fit the person to the job*. Whether using a "model" for the basis of an analysis, or just looking for some kind of structure to help get started, there are several relevant categories that must be understood when trying to apply ergonomic interventions:

- The People Involved: How do people interact and behave in groups in relation to the work process and task?
- The Tools and Technology: How are tools and technology used? How do they affect the users' ability to do their job?
- The Organization: How does the organization affect the workers' ability to do their job?
- The Work Processes: How do the written procedures and norms affect people, and the quality of the work products?
- The Task: How does the task affect the worker's ability to do their job?
- The Environment: What effect does the physical environment have on the workers and the job?

Ergonomic and process improvements are also linked to the other elements of the Human Factors program. Just as a complete incident analysis may provide input to be linked to Human Factors training, input may also be directed toward procedure improvements, Ground Support Equipment modifications, hardware repairs, policy changes, design of job aids, assessments of Personal Protective Equipment (PPE), etc.

Evaluation of the effectiveness of the ergonomic interventions or process improvements must be tied to reliable organizational metrics to monitor success and progress. If the chosen metrics do not reflect the desired results after a satisfactory time period has passed, then either the implementation or the strategy itself should be re-evaluated. The risk of this approach is that a continuous "de-stabilization loop" is established that may have negative system effects.

Finally, feedback is an essential element in the constant cycle of evaluation and improvement. Similar to other elements of a human factors program, feedback must be honest, timely, and acted upon in order for the program to be credible. The same holds true for feedback provided as part of the ergonomic intervention or process improvement. Where there is increased safety of people, or reduction in injury potential, then the feedback may be generated from the local area to the rest of the organization. Where the benefit is more system-wide in nature (as reflected in some organizational metric) then the feedback may be generated from a centralized management level out to the local workgroups. Either way, it is important to recognize that feedback is part of a continuous loop.

## **Safety Metrics**

### Human Error Database

Basic elements of the error management process include: maintenance error reporting and investigations; error and contributing factor data analysis; and the implementation and validation of error prevention strategies based on investigation results<sup>29</sup>.

Given the elements above, the human error database should be organized so that:

- Human error information associated with events can be easily retrieved and reported
- Causal chains and contributing factors associated with events can be clearly represented
- Data can be summarized to show patterns and trends
- Database is organized so that investigation, analysis and corrective action tracking can be linked

Safety metrics based a richly populated human error database can provide the key to identifying and understanding maintenance human error. Furthermore, when the database contains information that is reliably gathered and systematically organized, analyses can reveal patterns that point to systemic problems and trends over time. In some cases, safety metrics not only indicate potential risks but point toward intervention strategies. A linked database can then track corrective action progress.

But the real challenge in maintaining a human error database is not the database tools; rather it is cultivating and maintaining a work environment in which communication is open is honest; where members of the workforce do not feel their jobs are in jeopardy or where individuals are uncertain about safety priorities. (whether perceived or actual). Individuals will simply NOT provide information about errors if they feel this action puts their jobs at risk. In an organization experiencing downsizing and extreme re-structuring exercises, it is particularly difficult to maintain a "worry-free perspective".

Therefore there is an uncertain relationship between error data and safety. Under some conditions, fewer errors reported corresponds to fewer errors committed, and thus, they are indicators of less safety risk. Under other conditions, fewer errors reported simply means people are reluctant to report. The correspondence of number of errors reported and number of errors committed is unknown. Thus, the interpretation of safety metrics is problematic, and requires a sensitive understanding of the day-to-day workplace climate. Analysts must be aware of perturbations in the system; further, they must understand how perturbations affect safety metrics. Finally, in order to use safety metrics in making management decisions, there must be clear baselines that have been benchmarked in the industry.

On the other hand, individual cases within an error database are also valid as single cases. Even when trends and patterns are elusive, there are lessons that can be learned and errors to be understood from a single case study. For instance, one can learn a great deal about human error from one accident that is thoroughly investigated. One can learn other kinds of lessons from large, self-report databases that lack detail but represent a more representative sampling of cases. Finally, a human error database within an organization can provide valuable information about interventions needed, and trends that can be avoided. But most important, the collection of open, honest data must occur in order to have confidence in the value of the data.

### Effectiveness of Human Factors Interventions

Safety metrics are also important in evaluating the effectiveness of corrective actions and intervention/prevention strategies. It is important to identify or develop valid and reliable processes for measuring the effectiveness of one's actions. For example, in order to evaluate training effectiveness, pre-training baselines are needed for making post-training comparisons. Because there are multiple ways to assess program effectiveness, it is advantageous to collect a variety of measures when possible.

Measurement data may be acquired through various means: surveys, observations, and existing organization metrics (e.g., on-the-job injuries, ground damage incidents). These measures may represent immediate or longer-term effects; they may be self-report measures of attitudes, intentions, and beliefs or they may be more objective measures of individual behaviors and group performance outcomes. The state and availability of

**SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT**  
**FEBRUARY 9, 2000**

---

safety measures varies from airline to airline in the U.S. In some cases top maintenance management interest in a set of performance outcomes (many of them with safety implications) can create manifest availability and visibility. It should be noted that safety measures will only be available if management is directly and continuously interested in receiving them. A further issue is universal or standard safety metrics. In this regard it is clear that what is defined, as "of interest" for one airline is not common across the industry.

## Appendix 4B: 1998 Aerospace Safety Advisory Panel (ASAP) Human Factors Summary

Table 7 -- ASAP Findings and NASA Responses

Discussion Points	
ASAP Finding & Recommendation #1	NASA Response #1
<p><b>Finding:</b> Loss of core competencies due to budget and personnel ceiling constraint</p> <p><b>Recommendation:</b> Provide Kennedy Space Center, Johnson Space Center, Marshall Space Flight Center with budgetary resources and administrative flexibility needed</p>	<p>Provision of relief to Office of Space Flight Centers in FY00</p> <ul style="list-style-type: none"> <li>• Enable innovative use of temporary &amp; extended term appointments</li> <li>• Increase permanent hours to fill critical skill positions</li> <li>• Additional relief as identified by Core Capability Assessment</li> </ul>
ASAP Finding & Recommendation #2	NASA Response #2
<p><b>Finding:</b> Shortfalls in workforce training within both NASA and USA, caused by downsizing; related difficulty in hiring to fill skill shortage</p> <p><b>Recommendation:</b> NASA and USA to review critical skills and certification requirements and institute programs</p>	<p>Critical skill review and requirements completed; quality initiatives developed for:</p> <ul style="list-style-type: none"> <li>• Cross training, automated training tools</li> <li>• On-line automated certification validation</li> <li>• Enhancement to the closed loop verification of operations and system operational performance</li> </ul>
ASAP Finding & Recommendation #3	NASA Response #3
<p><b>Finding:</b> Combined effect of downsizing, hiring freeze and Shuttle Flight Operations Contract transition may lead to lack of hands-on technical knowledge and experience in senior management</p> <p><b>Recommendation:</b> Training and career paths to focus on hands-on technical knowledge and experience</p>	<p>Concurrence with ASAP</p> <ol style="list-style-type: none"> <li>1. Obtain operational experience through audit, surveillance, partnering, direct observations, etc.</li> <li>2. Succession planning and preparation for next generation supervisors, managers and senior management positions</li> <li>3. NASA training philosophy to emphasize on the job training supplemented by classroom instruction, participation in outside programs</li> <li>4. Training budget has provide increase of 20% for Office of Space Flight from FY 1997-2000</li> <li>5. New initiatives: NASA Academy of Program and Project Leadership, etc.</li> </ol>

Table 8 -- ASAP Findings and NASA Responses (cont.)

**SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT**  
**FEBRUARY 9, 2000**

Discussion Points	
ASAP Finding & Recommendation #4	NASA Response #4
<p><b>Finding:</b> Difficult to find meaningful metrics that directly show safety risks/unsafe conditions; should learn more from mishaps and close calls</p> <p><b>Recommendation:</b> In addition to standard metrics, NASA should be aware of mishaps/close calls, follow-up in timely matter, concur on corrective actions</p>	<p>Concurrence with ASAP</p> <ul style="list-style-type: none"><li>• HF Integration Office, NASA/contractor HF IPT; Analysis of root cause and contributing cause data across all Kennedy Space Center</li><li>• Expand definition of "close call", quarterly reviews, shift paradigm from negative aspect</li></ul>
ASAP Finding & Recommendation #5	NASA Response #5
<p><b>Finding:</b> A principle cause of Space Shuttle processing errors is incorrect documentation</p> <p><b>Recommendation:</b> NASA and USA must place increased priority on determining error sources</p>	<p>Concurrence with ASAP</p> <ul style="list-style-type: none"><li>• Estimated metrics to identify types and sources of documentation error. Implemented check and balance in work instruction generation process.</li><li>• NASA/USA initiative to reduce complexity or work procedures and process for making changes, increase standardization</li><li>• USA developing integrated on-line system that ensures total process rigor and mitigates potential for human error incorporated "best practices" for authoring, etc.</li><li>• Goal of above activity to ensure properly certified personnel utilizing the right work instructions</li></ul>

## Appendix 4C: Aerospace Advisory Panel – Discussion

### Aerospace Safety Advisory Panel Findings

In Appendix 4B: 1998 Aerospace Safety Advisory Panel (ASAP) Human Factors Summary, the Aerospace Safety Advisory Panel findings covering 1989-1998 have been summarized into several categories: Reporting and Tracking, Operations, and Workforce. Human Factors issues appear often within these categories. For example, through 1995, general human factors issues are discussed in terms of resolving safety problems, and improving spaceflight and ground operations. The specific issue involving the development of fatigue countermeasures is mentioned as well as the incorporation of human factors into the system of incident/mishap reporting and investigation.

From 1996 onward, workforce issues attract continual attention with respect to downsizing and the transition to the Shuttle Flight Operations Contract. The Review of Issues Associated with Safe Operation and Management of the Space Shuttle Program (11/96) is particularly relevant. The “management of independent safety oversight” and “downsizing” concerns predict problems that continue to raise concerns (e.g., ability to continue on-site surveillance, maintaining an appropriate skill and experience mix, clarity of institutional future post FY00 for Kennedy Space Center, and clarity of NASA’s responsibility vis a vis the contractor).

With respect to reporting and tracking findings, human factors issues pre-1995 focus on incident and mishap reporting as well as procedural problem tracking and deficiencies. Post-1995 human factors issues focus on safety and quality, the effects of downsizing, and a return to documentation problems (see **Problem Reporting & Tracking Process**).

Finally, human factors are also involved in the category of “Operations” findings. The issue of “Safety First” recurs in 1990, 1993, 1997 and 1998. Through 1995 human factors operational concerns discuss the need for improved processes and teamwork as well as some very specific Thermal Protection System and Space Shuttle Main Engine needs. From 1995, the focus is on cutbacks, transition of responsibility and reduced NASA presence on the floor.

Because of the significance of the Aerospace Safety Advisory Panel findings to SIAT concerns, we have considered the 1998 Report (<http://www.hq.nasa.gov/office/codeq/codeq-1.htm>) in more detail. Human factors issues are directly concerned in Aerospace Safety Advisory Panel Findings #1-5 discussed below. However, some general commonalities shared by the Aerospace Safety Advisory Panel and SIAT are the following:

1. a similarity of issues (e.g., concern with core competencies, skill mix, cross-training),
2. a recognition that downsizing and transition to the Shuttle Flight Operations Contract are primary sources of a variety of concerns. In addition, similar to Aerospace Safety Advisory Panel methods, the SIAT used an interview approach for collecting observations from personnel in a closed-door, non-threatening session.

Differences between the Aerospace Safety Advisory Panel and SIAT are notable as well. First, Aerospace Safety Advisory Panel site visits and interviews have been conducted for many years on a regular basis, and across the full Shuttle system. This provides a longitudinal history of observations that can be interpreted within a system-wide context over time. SIAT observations and interviews are necessarily a snapshot in time. While the SIAT sampled a variety of jobs and affiliations, there was by no means system-wide sample representation. However, what we lack in a historical interpretative context, we hope to gain in having an independent perspective (see **Appendix 4B: 1998 Aerospace Safety Advisory Panel (ASAP) Human Factors Summary**).

## **Parallels to Aerospace Safety Advisory Panel Findings**

### Aerospace Safety Advisory Panel Finding #1: Loss of core competencies

Aerospace Safety Advisory Panel 1998 Finding #1 is that NASA is moving in the direction of crisis-level loss of core competencies due to budget and personnel ceiling constraints. The Aerospace Safety Advisory Panel recommends that budget resources be provided the Office of Space Flight Centers (Kennedy Space Center, Johnson Space Center and Marshall Space Flight Center) and the administrative flexibility they need to use the resources. NASA's response is that they are providing the resources to the Office of Space Flight Centers in FY00 to enable them to make innovative use of temporary and extended term appointments and increase permanent hours to fill critical skill positions. Additional relief will be provided as identified by the Core Capability Assessment.

The SIAT observations are consistent with Aerospace Safety Advisory Panel Finding and Recommendation #1. However, several lingering concerns are the following.

1. Because of its proximity to the safety margin, Shuttle operations should take precedence over competing programs within NASA Centers. Furthermore, priorities based on mission safety should consider human factors concerns as indicated by existing incident analyses (e.g., USA Human Factors Team) and should solicit input from the workforce to identify areas of maintenance error vulnerability. Even if some functions are no longer considered to be "NASA" responsibility, safety concerns must be addressed; in some cases, roles and responsibilities may need to be clarified. A recent Independent Assessment<sup>30</sup> states this concern in a slightly different way. They state that the Shuttle Processing Directorate workforce believes that Kennedy Space Center management wants to cease operations work and concentrate on R&D immediately. If this is not true (as the SIAT states most emphatically it is not), we are less concerned that the budget resources could be re-directed away from the most immediate safety issues.
2. Hiring new personnel is initially a liability. In addition, training to certification is not equivalent to gaining on-the-floor experience. Therefore acquiring additional workforce to fill critical skill positions will not provide immediate relief. Performance expectations should fit the skills and resources of the workforce, acknowledging that certification and years of experience do not automatically equate experience in a new work area or new work role.
3. Although hiring and training new personnel are logical steps toward making up for the loss of core competencies, these are slow processes and initially add to the workload of existing personnel. Innovative avenues for restoring experience in safety critical areas should be explored.

### Aerospace Safety Advisory Panel Finding #2: Shortfalls in workforce training

Aerospace Safety Advisory Panel 1998 Finding #2 refers to the shortfalls in workforce training within both NASA and USA, caused by downsizing activities. They discuss the related difficulty in hiring to fill skill shortage. The Aerospace Safety Advisory Panel recommends that NASA and USA review critical skills and certification requirements and institute programs to alleviate these problems. NASA responds that the critical skills and certification review and requirements has been completed. Quality initiatives have been developed for cross-training and automated training tools, inline automated certification validation, and enhancements to the closed loop verification of operations and system operational performance.

The SIAT observations are consistent with Aerospace Safety Advisory Panel Finding and Recommendation #2. The NASA response incorporates initiatives that should be helpful. The question is whether these initiatives are adequate for all skill shortages and how long it will take before there is a significant improvement.

1. Some members of the workforce told the SIAT that "cross training" was a not a planned learning activity; rather it was a way to "borrow" people when an area had a skill shortage. Clearly both perspectives may contain some truth, but our concern is whether cross training is implemented to maximize the training opportunity and whether it is conducted in preparation for skill needs.

2. The new technologies mentioned may support some types of training needs and they may improve some processes, but they can never substitute for on-the-job training (OJT) and appropriate partnering of inexperienced with the experienced.

Aerospace Safety Advisory Panel Finding #3: Lack of hands-on technical knowledge and experience

Aerospace Safety Advisory Panel 1998 Finding #3 discusses how the combined effect of downsizing, hiring freeze and the Shuttle Flight Operations Contract transition may lead to a lack of hands-on technical knowledge and experience in senior management. They recommend that training and career paths focus on hands-on technical knowledge and experience. NASA concurs with the Aerospace Safety Advisory Panel finding and recommendation #3 and brings forth a number of actions to be taken. Among these are the following:

1. Obtain operational experience through audit, surveillance, partnering, direct observations, etc.
2. Succession planning and preparation for next generation supervisors, managers and senior management positions
3. NASA training philosophy to emphasize on the job training supplemented by classroom instruction, participation in outside programs
4. Training budget has provided an increase of 20% for Office of Space Flight from FY1997-2000
5. New initiatives such as the NASA Academy of Program and Project Leadership, etc.

The SIAT observations are consistent with the Aerospace Safety Advisory Panel Finding and Recommendation #3, and the NASA response contains many good actions. Nevertheless, a few concerns are raised. For example, how has the increase in training budget been used and what will happen beyond FY2000? Has the training been consistent with the new NASA philosophy? Some workforce perceptions would indicate training has not kept pace with the changes and work demands; and that preparation for the future has advanced at the expense of current Shuttle operations. Stating a NASA training philosophy that emphasizes on the job training supplemented by other training variants is an excellent response although there is always the danger of adding requirements that cannot be fully implemented due to resource and scheduling limitations

Aerospace Safety Advisory Panel Finding: #4: Meaningful safety metrics

The Aerospace Safety Advisory Panel 1998 finding #4 focuses on the difficulty of finding meaningful metrics that directly show safety risks or unsafe conditions. It further points out that NASA should learn more from mishaps and close calls. They recommend that in addition to standard metrics, NASA should be more aware of mishaps and close calls, follow up in a timely manner and concur on corrective actions.

It is pointed out in the NASA response that the NASA Human Factors Integration Office, and the NASA/contractor Human Factors Integrated Product Team are currently tasked with conducting analyses of root cause and contributing cause data Kennedy Space Center-wide. In addition they will expand the definition of "close call", conduct quarterly reviews and initiate a shift in paradigm away from the negative aspects of investigating human error.

The SIAT observations are consistent with the Aerospace Safety Advisory Panel Finding and Recommendation #4.

- The SIAT strongly supports the current NASA and contractor human factors initiatives described above. However, the usefulness of these efforts are limited and need greater support and resources. For example, close call voluntary reporting is predicated upon an organizational climate where personnel are confident of a "just culture". As experienced in the aviation industry and others, this is a condition that requires vigilant monitoring.
- A paradigm shift is a slow and fragile process and cannot be maintained with a simplistic one-time solution. Unfortunately, a Safety Culture cannot be created through decree but through painstaking, long-term solutions<sup>31</sup>.



**SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT**  
**FEBRUARY 9, 2000**

The SIAT was provided a sample of how the Kennedy Space Center Shuttle Processing Human Factors Team investigates and analyzes human error events. The level of understanding and rigor with which the team organized information and identified elements of the causal chain and associated contributing factors was impressive. Although the number of events investigated is small, the analysis process is an excellent model. Unfortunately, only 7 of 14 Incident Error Review Board events and 15 of 78 Shuttle Operations Assessment Group events were analyzed for all of FY99.

The Shuttle Processing Human Factors Team has been analyzing events since FY96; hence they have been able to examine some trending of factors. Given an appropriate number of cases, trending analyses are very useful for identifying human error vulnerabilities. For example, one contributing factor is called "Lack of Task Specific Experience". This refers to cases where individuals have been assigned to a task for which they minimal to no target task experience. In some cases, there was not the appropriate paring up with an experienced partner. In other cases, the engineer or quality inspector was either inexperienced in that area or were simply not available. Considering the extent to which this factor has been implicated in Incident Error Review Board (IERB) events (incidents in which there is more than \$1000 damage or serious personnel injury from FY96-FY99, "Lack of Task Specific Experience" has played a key role.

**Table 9 -- Role of "Lack of Task Specific Experience" in IERB Events, FY96-99**

<b>FACTOR: "Lack of Task Specific Experience"</b>		
<b>Year</b>	<b>Number of Occurrences/ Total IERB* events</b>	<b>Per cent Occurrences</b>
FY96	4/12	33%
FY97	2/8	25%
FY98	5/11	45%
FY99	4/7	57%
*NOTE: IERB events: More than \$1000 damage or serious personnel injury		

In short, the relative contribution of this factor to maintenance error is increasing. Although the numbers are small, this slight trend confirms the Aerospace Safety Advisory Panel findings and observations made by the SIAT.

This simple example highlights one way in which a bigger investment in human factors safety metrics may facilitate the effective implementation of corrective actions. The NASA Safety Incident Log for FY99 contained 52 events in which about 60% involved workmanship issues and 40% involved hazards in the workplace. Apart from sheer volume, it is notable that most of these events could benefit from a more complete analysis. In a different but probably overlapping another listing of mishaps, incidents and close calls for FY99 (provided in SIAT response #60), a total of 57 events are identified. By any count (the numbers vary according to which database is cited), the SIAT observes only 7 Incident Error Review Board events and 15 Shuttle Operations Assessment Group events analyzed for Human Factors in FY99.

Clearly, great potential exists for enhancing the definition of safety metrics. Rather than stopping at the mere categorization of factors such as "workmanship" or "workplace hazards", analyses such as those conducted by the Shuttle Processing Human Factors Team should be considered more seriously, and used as a model for investigating and assessing as many mishap, incident and close call events as possible.

**Aerospace Safety Advisory Panel Finding #5: Processing errors due to incorrect documentation**

Aerospace Safety Advisory Panel 1998 Finding #5 states that a principle cause of space Shuttle processing errors is incorrect documentation. They recommend that NASA and USA must place increased priority on determining error sources. The NASA response discusses their attempt to estimate metrics to identify types

**SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT**  
**FEBRUARY 9, 2000**

---

and sources of documentation error, and further notes the implementation of checks and balance in work instruction generation process. NASA/USA initiatives have been undertaken to reduce the complexity of work procedures and processes for making changes, and increase standardization.

The SIAT observations are consistent with the Aerospace Safety Advisory Panel Finding and Recommendation #5. However, several concerns are raised with respect to parts of the NASA Response:

- Although ensuring process rigor is possible, human error can never be completely mitigated. There must be continuing vigilance for identifying and taking proactive measures against human error potential.
- "Ensuring properly certified person" must be defined within the context of the new training philosophy. "Certification" does not discriminate among differences in levels of experience nor does it recognize the importance of appropriate skill mix within teams. Finally, do work instructions incorporate the necessary input from on-the-floor expertise?

## Appendix 5

### Hydraulics: Additional Information

#### Background

##### Maintenance Requirements

Shuttle maintenance requirements, including every flight and major down periods, are determined by the "Operations and Maintenance Requirements and Specifications Document (OMRSD)." This document is authorized by the requirements of NSTS 07700, Space Shuttle Flight and Ground System Specification.<sup>32</sup> File III of the Operational Maintenance Requirements and Specifications Document defines what maintenance shall be performed at the Orbiter system level, V58 for the hydraulic system, based on the Master Verification Plan (MVP). The Master Verification Plan identifies the Turnaround Validation and Checkout Requirements based on the likelihood (probable, infrequent, remote and improbable) and severity (criticality 1, 1R, 1S, 2, 2R and 3) of a component failure.

Changes in Orbiter maintenance requirements start with the Prevention/Resolution Team where rationale for the change is discussed and formulated. Once the team has decided on a particular change, it is submitted via a Requirements Change Notice (RCN) for all Prevention/Resolution Team members to comment on and then presented to the PRCB (Program Requirements Control Board) for approval. Hydraulic system Prevention/Resolution Team members include NASA, USA and Boeing. For a maintenance requirement non-compliance (waiver), approval is required by the systems level engineers (Kennedy Space Center NASA, USA and Boeing), chief engineers (Kennedy Space Center NASA/USA/Boeing) and the NASA Program Requirements Control Board chairman. If the compliance is not technically acceptable to any member, the hardware will be replaced.

Aircraft operated by the commercial freight carrier Federal Express follow a maintenance plan called the "Baseline." This baseline is established by Boeing (using the Maintenance Steering Group approach), the Federal Aviation Administration (FAA) and the freight carrier itself and provides directions as to the detail of inspections and tests during scheduled maintenance. Maintenance can consist of A (line), B (90 day) or C (15 month) checks, increasing in complexity and vehicle intrusiveness as the time span increases from the last C check. Component failure data, which is tracked and analyzed by a reliability group, has led the carrier to make conservative changes to the Baseline requiring more maintenance during regularly scheduled checks. These changes are driven by economics, since it keeps aircraft in the air longer requiring less costly maintenance between the scheduled checks. Non-compliance of requirements requires Boeing and Federal Aviation Administration approval.

General maintenance requirements for the B-2 bomber program, called Tech Orders, originated with the manufacturer Northrop-Grumman and were validated by the Air Force. Changes to the Tech Orders or non-compliance require Air Force signature.

## Appendix 6

### Hypergols and Auxiliary Power Unit: Additional Information

#### Background

##### Maintenance Requirements

Shuttle maintenance requirements, including every flight and major down periods, are determined by the Operations and Maintenance Requirements and Specifications Document. This document is authorized by the requirements of NSTS 07700 Space Shuttle Flight and Ground System Specification.<sup>33</sup> File III of the Operational Maintenance Requirements and Specifications Document defines what maintenance shall be performed at the Orbiter system level (V42 for Reaction Control System, V43 for Orbiter Maneuvering System and V46 for Auxiliary Power Unit) based on the Master Verification Plan. The Master Verification Plan identifies the Turnaround Validation and Checkout Requirements based on the likelihood (probable, infrequent, remote and improbable) and severity (criticality 1, 1R, 1S, 2, 2R and 3) of a component failure.

Changes in Orbiter maintenance requirements start with the Problem Resolution Team where rationale for the change is discussed and formulated. Once the team has decided on a particular change, it is submitted via a Requirements Change Notice for all Prevention/Resolution Team members to comment on and then presented to the Program Requirements Control Board for approval. Orbital Maneuvering and Reaction Control System or Auxiliary Power Unit Prevention/Resolution Team members include NASA, USA and Boeing. For any maintenance requirement non-compliance (waiver), approval is required by the systems level engineers (Kennedy Space Center NASA, USA and Boeing), chief engineers (Kennedy Space Center NASA/USA/Boeing) and the NASA Program Requirements Control Board chairman. If the compliance is not technically acceptable to any member, the hardware will be replaced.

Maintenance requirements, otherwise known as Tech Orders, for F-16 aircraft flown by NASA at the Dryden Flight Research Facility (DFRC), are determined by the Air Force and originated with the manufacturer. System engineers may add maintenance requirements in order to verify the integrity of certain components beyond the manufacturer's recommendation. The Chief of Flight Operations, a government employee, must approve any changes, additions or waivers to the Tech Orders.

The Acceptance Checkout Retest and Backout (ACRBC) document sets the system level maintenance requirements for the Titan 4-B program. This document receives inputs directly from the hardware vendor, which is then incorporated into documentation by Lockheed-Martin in Denver. LM approval is only required for minor Acceptance Checkout Retest & Backout changes. The Titan 4-B program requires several levels of approval for repairs and fly as-is non-conformances, yet government approval is required only if the non-compliance affects performance characteristics or major design features of the vehicle.

## Appendix 7

### Propulsion: Additional Information

#### Background

##### Space Shuttle Main Engine

The Orbiter vehicle main propulsion system includes three Space Shuttle Main Engines (SSMEs). A Space Shuttle Main Engine is a reusable, high-performance, liquid-propellant rocket engine with variable thrust. All three engines are ignited on the ground at launch, operating in parallel with the solid rocket boosters during the initial ascent phase, and continuing to operate for approximately 510 to 520 seconds total firing duration. Each engine operates at a mixture ratio (liquid oxygen/liquid hydrogen) of 6:1 and a chamber pressure of approximately 3,000 psia to produce a sea level thrust of 375,000 pounds and a vacuum thrust of 470,000 pounds. The engines are throttle able over a thrust range of 65 to 109 percent of the rated power level. This provides a higher thrust level during lift-off and the initial ascent phase, and allows Orbiter acceleration to be limited to 3 g's during the final ascent phase. The engines are gimballed to provide pitch, yaw, and roll control during Orbiter boost phase.

The Space Shuttle Main Engines' very high performance is enabled by the use of a staged combustion power cycle coupled with high combustion chamber pressures. In the Space Shuttle Main Engine staged combustion cycle, the propellants are partially burned at low mixture ratio, very high pressure, and relatively low temperature in the pre-burners to produce hydrogen-rich gas to power the high-pressure turbopumps. This hydrogen-rich steam is then routed to the Main Injector where it is injected, along with the LO<sub>2</sub> oxidizer and some additional H<sub>2</sub> fuel, into the main combustion chamber at high mixture ratio and high pressure. Hydrogen fuel is used to cool all combustion devices that are directly exposed to contact with high-temperature combustion products. An electronic engine controller automatically performs checkout, start, mainstage, basic operational, and engine shutdown functions.

The Space Shuttle Main Engine is unique. While a few other engine designs throughout the world have used the staged combustion cycle to maximize thrust to weight ratio and specific impulse, no other liquid fueled booster engine is reusable. The reusability requirements place unique requirements on the engine design, processing, test, and maintenance. Low and high cycle fatigue, fracture mechanics flaw detection and growth rate, and engine repair and maintenance between flights become design and operations drivers.

The Space Shuttle Main Engine first flew on Shuttle Columbia 18 years ago and has successfully delivered 95 Shuttle crews to orbit. A key safety advantage inherent in the Space Shuttle Main Engine is its ability to be tested repetitively. Before the first flight, two engines were each required to operate 20,000 seconds without failure or significant defects. Furthermore, component life is established and paced by the Fleet Leader Concept, which requires successful hot fire ground test of every generic flight component to twice the flight life limit.

Rocketdyne designs, builds, tests, and maintains the Space Shuttle Main Engines. The Rocketdyne team operates in an integral manner with the Marshall Space Flight Center team. Many of the joint team members have ten to twenty years experience on the Space Shuttle Main Engine program. This experience based "corporate" memory/knowledge, and the inherent value of continuous responsibility of the Original Equipment Manufacturer (OEM) have been a great asset.

Over the life of the program, Rocketdyne has taken great pride in maintaining a successful program. The quality of engineering and design is matched by the hands-on technicians who test, repair, and maintain the engines.

## Engine Upgrades

The Space Shuttle Main Engine has been continuously improved throughout the program. Early significant changes have included the controller, temperature, and pressure instrumentation, nozzle, Main Injector liquid oxygen posts, spark igniter, and increased redline protection. Recent major safety upgrades resulted in two block changes.

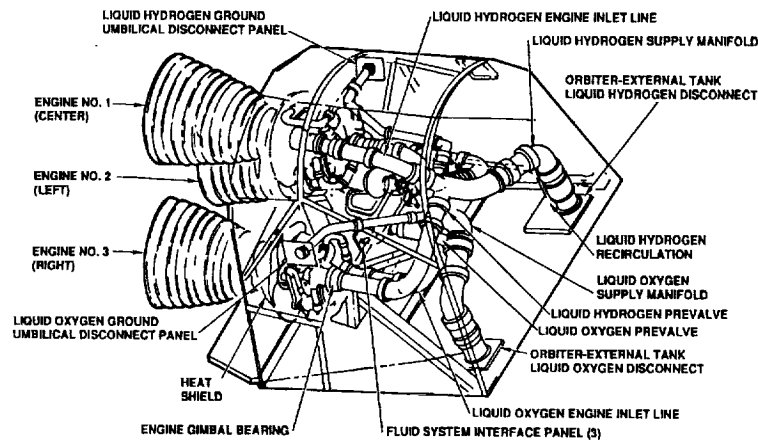


Figure 31 -- Space Shuttle Main Engine

### Block I

#### Alternate High Pressure Oxidizer Turbopump (HPOTP/AT):

The original high pressure oxygen pump operated safely over many flights and ground test firings; however, it required disassembly and replacement of the bearings every third flight. This pump was designed when every ounce of weight was considered significant to meeting Shuttle performance requirements. With improvements to Shuttle performance, it was possible to allocate increased weight to the pump for safety enhancement. With the inclusion of these safety enhancements, the Alternate High-Pressure Oxidizer Turbopump weighs 741 pounds or 166 pounds more than the original pump. The main safety improvements fall into two categories.

The turbine shaft and the two turbine discs are integral and extremely robust. Likewise, the bearings are robust and allow nine flights between overhauls. The turbine blades are hollow, which minimizes the unbalance of the rotating assembly if blade damage occurred. These factors greatly reduce the possibility of pump housing failure, which would result in a criticality-one situation.

The original pump housing is made up of welded parts. Many of the internal welds cannot be inspected for cracks, which is required for fracture mechanics verification that critical flaw growth is not occurring. Other than inspection, the other approach to fracture mechanics is to screen out critical flaws with a proof test (as done with the External Tank). The Alternate High-Pressure Oxidizer Turbopump housing eliminated all uninspectable welds (reduced from 250 to 0). The total number of welds was reduced from 300 to 7 through the use of fine grain castings. The bolted assembly can be disassembled for inspection.

#### Two Duct Powerhead

The original hot gas manifold, which feeds hydrogen rich exhaust gases from the fuel pump pre-burner into the Main Combustion Chamber (MCC) used three ducts to transport these gases. Early in the program, there were failures of Main Combustion Chamber liquid oxygen posts due to the extreme loading caused by hydrogen impingement. Water flow tests showed that the center duct flow was extremely low, making this duct ineffective. The center duct flow deficiency caused the two adjacent ducts to carry more flow than intended resulting in high impingement pressure on the liquid oxygen posts.

The redesign eliminated the center duct and increased the flow area of the other ducts, reducing duct pressure and liquid oxygen post impingement pressures.

#### Single Tube Heat Exchanger

Oxygen used to pressurize the External Tank is heated by the High Pressure Oxidizer Turbine discharge. The original heat exchanger had bifurcated tubes. That is, two tubes were manifolded together at the inlet and outlet of the heat exchanger, involving multiple welds in the tubes.

The new design replaced the bifurcated tubes with a single tube of increased wall thickness. This eliminated the welds inherent in the original design. A leak in the heat exchanger is criticality-one

#### High Reliability Sensor/Controller

The controller is a fully redundant dual channel digital device, which provides continuous closed-loop mixture ratio and thrust control while also monitoring all engine health and redline functions every 20 milliseconds. The Block II controller (implemented in 1992) incorporated significant improvements in space-rated electronics and has an extremely high reliability (Mean Time Between Failures of 1 in 14,000 hours). All critical performance and redline monitoring sensors have also been upgraded. The High Pressure Fuel and Oxidizer Turbine Temperature redline sensors, which were originally resistance temperature devices utilizing a small (0.9 mill) platinum wire have been replaced with robust quad-redundant thermocouples. The pressure sensors were redesigned to eliminate internal conductive contamination. An advanced x-ray and ultrasonic inspection technique was also developed to verify integrity. Numerous software logic improvements were developed to provide increased reliability through enhanced redundancy management and sensor qualification.

### **Block IIA**

#### Large Throat Main Combustion Chamber

The main advantage in the Large Throat Main Combustion Chamber (LTMCC) is that the increased throat area reduces temperatures and pressures in combustion chambers, pumps, liners, etc. For example, fuel pump turbine discharge temperature was reduced about 120°F. This allowed reduction of the redline discharge temperature so as to give greater margin of safety for contingency engine shut down. It is estimated that this 2X increase in engine reliability did cost about 1.5 seconds of specific impulse, since the nozzle area ratio was reduced from 77 to 69.

#### High Pressure Fuel Turbopump

Many internal sheet metal welds were eliminated by using Electrical Discharge Machining to manufacture the turbine inlet as a complete unit, rather than by welding individual pieces together.

#### Low Pressure Oxidizer Turbopump

Silicon Nitride bearing balls were used to replace the 440C stainless steel bearing balls. These bearings have proved in testing to be much more resistant to wear and spalling than the steel bearing balls.

### **Block II**

Block II upgrades encompass all the Block IIA upgrades, but adds an alternate High Pressure Fuel Turbopump (HPFTP/AT). In fact, Block IIA was not planned but was implemented as an interim step to allow comprehensive resolution of Alternate High-Pressure Fuel Turbopump development issues. The safety advantage of the Large Throat Main Combustion Chamber was considered to be important enough to be put into the flight program without delay.

**SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT**  
**FEBRUARY 9, 2000**

---

The Alternate High-Pressure Fuel Turbopump has the same robust design as the Alternate High-Pressure Oxidizer Turbopump described earlier. That is, it has integral shaft and disc, hollow blades, and robust bearings. There are no welds on the Alternate High-Pressure Fuel Turbopump and fracture mechanics inspection is utilized. The pump weights 1065 pounds, which includes a weight increase of 295 pounds over the pump it replaces.

About 100,000 seconds of test time has been accumulated during the development program. There have been three instances of blade damage during development with continued safe operation, which verifies that the pump can suffer major internal turbine damage and still contain the damage within the pump. This is of particular importance since the fuel pump turbine is usually the first component to fail as a result of any problem within the engine which causes the oxygen fuel ratio to exceed the 6:1 design value, such as a nozzle leak.



## Appendix 8

### Risk Assessment & Management: Additional Information

#### Background

##### SSP Risk Management Process

SSP risk management activity is mainly conducted according to a set of an overall program requirements and procedures documents.<sup>34, 35, 36</sup>

NSTS 08117 is the most important document that assures flight safety. It constitutes the main part of the SSP risk management process. The purpose of the NSTS 08117 document is to define the Space Shuttle Program (SSP) Flight Preparation Process (FPP). It defines the procedures for the project milestone reviews and the Flight Readiness Review (FRR). It also defines the endorsement documentation required at the completion of the Flight Readiness Review, which provides the Certification of Flight Readiness (CoFR) for flight. Some of the safety related activities/areas that are addressed as part of the Certificate of Flight Readiness process include Failure Modes and Effects Analysis and the Critical Items List (FMEA/CIL), Hazard Analysis (HA), Alerts, System Safety Review (SSR), Waivers, Problem Reporting and Corrective Actions (PRACA), Technical Issues, Safety and Mission Assurance independent assessment, and Program Review Boards.

Another important document that is related to safety is the NSTS 08171 Operational Maintenance Requirements and Specification document (OMRSD). The OMRSD is the single authoritative source for operations, maintenance, data and analysis requirements and specifications that are necessary to maintain and verify the system element, sub-system, or line replaceable unit/maintenance significant item operational readiness. The Operational Maintenance Requirements and Specifications Document is an important National Space Transportation System document because it supports the risk mitigation procedures addressed in the FMEA/CIL and Hazards Analysis.

The final example document is the NSTS 5300.4 (1D-2) document. It is a high level document intended to establish common Safety, Reliability, Maintainability, and Quality Assurance (SRM&QA) provisions for the SSP. This document is essential for the SSP risk management process because it defines the RMS&QA activities required by the SSP contractors.

## Appendix 9

### Software: Additional Information

#### Background

##### Flight Software Process<sup>37</sup>

Validation & Verification and Independent Validation & Verification are performed during 3 distinct phases of software development for the SSP: Definition, Development and Mission Preparation. USA is the principal performer for the Primary Avionics Software System (PASS) development and Boeing – Reusable Space Systems (RSS) is the principal performer for the Backup Flight System (BFS) development.

##### Definition Phase

This phase is comprised of the following steps:

1. Flight software needs

New Operational Increments (OIs), Flight Software modifications, mission data, new designs and Flight Software corrections begin with an expressed need defined by the SSP Flight Software community. These needs are identified through flight or mission plans, vehicle or equipment modifications, flight or ground crew requests, program directives or objectives, etc.

2. Needs analysis

The Flight Software community (SSP, Johnson Space Center Engineering, MOD, Crew Office, Shuttle Flight Operations Contract contractors, Kennedy Space Center, SR&QA, Independent Validation & Verification) performs analysis to determine if assessed needs should become program requirements and reports its recommendations through a Flight Software Change Proposal (FCP) to the Shuttle Avionics Software Control Board. If approved, a software Change Request is generated.

**Validation & Verification activity:** Accomplished through the system engineering analyses performed by Flight Software community. Once knowledgeable Flight Software community personnel determine a valid Flight Software requirement exists, a sponsor prepares the necessary change documentation.

**Independent Validation & Verification activity:** System engineering analyses performed by the Flight Software community are monitored informally.

3. Discrepancy Report (DR) analysis

Change Requests are analyzed to determine the appropriate disposition; the analysis includes determination of the need for a Flight Software requirement change.

**Validation & Verification activity:** Discrepancy reporting is performed by the continuous utilization, evaluation, and review of the operational Flight Software by the technical community. Flight Software Change Requests found are subjected to detailed systems engineering analysis to determine their criticality and validity. The Flight Software community software engineers evaluate the range of options available to correct the discrepancy and prepare the necessary disposition recommendations for action by the Shuttle Avionics Software Control Board.

**Independent Validation & Verification activity:** If a Change Request is generated as a result of the Shuttle Avionics Software Control Board or a Change Request is generated, change impact, S/W

requirements, and interface requirements analyses are performed and documented in an Software Independent Validation & Verification Report (SIR)

#### 4. Requirements Analysis

The Shuttle Flight Operations Contract evaluates the requirements and determines an approach to implement them. Once determined, the Shuttle Flight Operations Contract must evaluate the resources required for implementation and develop an implementation schedule. The Shuttle Flight Operations Contract is responsible for maintaining checklists and Change Request evaluation documentation for their respective processes, including desk audits/assessments and required engineering simulation requirements.

The Principal Function Manager's (PFM) organization accountable for the most significant change in the proposed Change Request is responsible for performing the necessary engineering simulations with the proposed Flight Software change, and reviewing the Change Request content and simulation results with the respective technical panel, e.g., GN&C panel, abort panel, etc. Shuttle Avionics Software Control Board representatives are responsible for developing an integrated position on Change Requests.

**Validation & Verification activity:** Flight Software community validates the interface compatibility and appropriate interactions between all the affected functions.

**Independent Validation & Verification activity:** Requirements generated will undergo a S/W requirements analysis and Interface requirements analysis with a report of findings going to the Shuttle Avionics Software Control Board. Any issues identified are reported to the responsible Change Request author either directly or at the Change Requests requirements inspection(s).

#### 5. Space Shuttle Program Authorization

The Shuttle Avionics Software Control Board is the forum for dispositioning proposed Flight Software changes. Membership includes: Shuttle Avionics and Software Office, Shuttle Systems Integration, Shuttle Flight Operations Contract, Johnson Space Center Astronaut Office, Johnson Space Center Mission Operations (operations and reconfiguration), Johnson Space Center Engineering (Avionics Systems Division), Johnson Space Center Safety, Reliability and Quality Assurance, Kennedy Space Center Shuttle Engineering and Payload Operations, and Independent Validation & Verification.

#### Development Phase

This phase is comprised of the following steps:

##### 1. Design, Code, Unit/Module Test

The Shuttle Flight Operations Contract uses separate groups to develop Flight Software in the Software Development Facility (SDF) with responsibility for all requirements analysis and programming. One group is responsible for developing the Flight Software for the new Operational Increment delivery and another group is responsible for verification testing of the Flight Software for the new Operational Increment delivery.

**Design:** Approved Change Requests contain requirement specifications that the new Operational Increment delivery is expected to provide. These requirements are the basis for Flight Software designs which the Shuttle Flight Operations Contract converts to detailed software designs which are documented in Detailed Design Specification (DDS) documents and review in design inspections.

**Code:** Upon completion of detailed design, the PASS or Backup Flight Software software developer then writes Flight Software code implementing the design and then reviewed at a Code Inspection. Less complex implementations sometimes combine the design and code inspections.

**Unit/Module:** Once code is completed, development (pre-build) tests are performed to verify equations, logic paths, range of values, and/or the module interface (Input/Output) performance. Development test plans are presented and reviewed at a Test Inspection.

**Validation & Verification activity:** Each activity has detailed written procedures which the Shuttle Flight Operations Contract's software quality assurance personnel monitor for compliance. All reviews and inspections are controlled by peer moderators, without management involvement other than oversight review and approval of Flight Software development standards and procedures. Design is inspected to

ensure that the design reflects both the stated requirements as well as intended requirement. Code is inspected to ensure conformity to Flight Software standards, prevent unintended functions, and control inefficient CPU/memory consumption. Tests are inspected to ensure that tests are performed at applicable levels of Flight Software development prior to beginning Flight Software integration via the load build process.

**Independent Validation & Verification activity:** A S/W design analysis is performed on the software design and code analysis is performed on the code. Results are documented in a Software Independent Validation & Verification Report. Areas of concern result in Change Request generation and are provided to the Shuttle Flight Operations Contract.

## **2. Load Build and System Test**

The Operational Increment development cycle is comprised of multiple load releases. Each Flight Software load release contains the preceding load release plus updates that have been completed during the development process (design, code, development test). As each load is being developed, functional testing is performed. After each load is built, system integration testing is done before release for verification testing. The object of these tests is to test functional interfaces, multiple functions, timing, system interface, and mission profile.

Each new load is released for detailed verification tests upon successful completion of the system tests. A subsequent test group begins performance verification tests when all the approved Change Request/Change Requests have been included in a load release at the First Article Configuration Inspection (FACI). The final development Operational Increment load release is known as the Configuration Inspection (CI) load.

**Validation & Verification activity:** The Shuttle Flight Operations Contract maintains responsibility for all Validation & Verification activities until the Configuration Inspection load is released. The Shuttle Flight Operations Contract's configuration management ensures that Flight Software modules are never added or changed unless proper authorization and procedures have been followed. The system integration tests conducted on each new load build consist of standardized system tests of the basic load characteristics and capabilities.

## **3. First Article Configuration Inspection**

First Article Configuration Inspection is a formal review milestone in the Operational Increment development template, and officially begins the verification phase of an Operational Increment. At this point, all Change Request/Change Requests have been incorporated into the First Article Configuration Inspection Verification load.

**Validation & Verification activity:** This is the first review in the Operational Increment development cycle where all elements of the Flight Software community participate. The review allows appropriate members of the Flight Software community to evaluate the Operational Increment status and determine if required development for all functions has been achieved.

## **4. Verification Test Procedure Reviews**

Two levels of testing are performed on operational hardware. Level 6 testing consists of module functional tests against requirements. Test analysts develop Verification Test Procedures (VTPs) to be used during testing. These are standard functional tests for Flight Software Principal Functions documented in Software Development Facility data sets; specific tests are selected or modified from these standards. New tests are prepared, as appropriate, by Level 6 test analysts to test new or modified functional capabilities.

Level 7 testing consists of integrated system performance tests against requirements and overall system performance. Generic Level 7 testing consists of Guidance, Navigation and Control System Integrity Tests, System Services Tests, and Vehicle Cargo Systems Tests.

**Validation & Verification activity:** The Level 6 Verification Test Procedure Inspections are conducted by the Shuttle Flight Operations Contract, with participation of the flight software community. They provide inputs, identify issues, and review test procedures. The Level 6 test procedures are approved by ASD for new development only. The Level 7 test specifications are reviewed in Test Coordination Team (TCT) meetings attended by interested parties from the Flight Software community. The resulting Level 7 Verification Test Specification is documented in a Change Request and formally approved by the Shuttle

Avionics Software Control Board. The object is to ensure that planned tests verify requirements as well as overall system performance.

**Independent Validation & Verification activity:** An analysis of the Verification Test program is documented in a Software Independent Validation & Verification Report and is provided to the Flight Software community.

#### 5. Functional Verification Testing

This activity is the execution of the Level 6 Functional Tests approved in the preceding activity. The Flight Software is functionally tested by exercising Flight Software Principal Functions affected during Change Request/Change Request implementation.

Level 6 Functional Tests are reviewed by the appropriate Flight Software community, and test results are accepted as a certification that the delivered software conforms to NASA approved requirements. Any Level 6 issues not closed are reported by the Shuttle Flight Operations Contract at the Configuration Inspection. Level 6 Epilogues (Test Reports) are published approximately six weeks after the Configuration Inspection and delivered to members of the Flight Software community upon request.

**Validation & Verification activity:** The Shuttle Flight Operations Contract is responsible for performing the tests according to the procedures and conditions approved in the verification test procedure. Functional tests are designed to examine the total functional range of specific principal functions provided by the Change Request/Change Requests implemented in the new Operational Increment. Detailed results from each Level 6 test case are evaluated by the technical community.

**Independent Validation & Verification activity:** Independent Validation & Verification performs analysis of the Level 6 test plans. Areas of concern are identified to the Shuttle Flight Operations Contract testing community.

#### 6. Performance Verification Testing

This activity performs the Level 7 Performance tests contained in the Verification Test Specification Change Request approved by the Shuttle Avionics Software Control Board, and normally begins with the delivery of the First Article Configuration Inspection Verification Load. Level 7 tests place emphasis on evaluating PASS or Backup Flight Software system performance instead of Flight Software Principal Functions, resembling flight profiles more closely than Level 6 tests.

**Validation & Verification activity:** By use of standardized generic Level 7 tests, each Operational Increment delivery is tested to the same specifications under the same conditions. New Capability Performance tests are designed to exercise the full envelope of capabilities provided by the specific Change Request/Change Requests implemented in the new Operational Increment. Participation of the Flight Software community in the Test Coordination Teams and Performance Test Reviews accomplish the Validation & Verification tasks during the design and conduct of tests.

**Independent Validation & Verification activity:** Independent Validation & Verification performs analysis of the Level 7 test plans. Areas of concern are identified to the Shuttle Flight Operations Contract testing community.

#### 7. Configuration Inspection

This is a formal review milestone in the Operational Increment development template at which the Shuttle Flight Operations Contract reports on Operational Increment development issues and Level 6/7 verification test issues, delivers updated Flight Software documentation, and releases the Configuration Inspection loads to NASA. This milestone officially completes the development phase of an Operational Increment.

After the Performance Verification Testing is completed, mission-based data sets are used to perform Operational Increment verification. This is the first integration of software and hardware-based emulators.

NASA is responsible for officially accepting the new Operational Increment from the Shuttle Flight Operations Contract. The Flight Software technical organizations are responsible for ensuring that their requirements have been adequately met.

**Validation & Verification activity:** The Configuration Inspection is preceded by Level 6 test results meetings and Level 7 Performance Test Review (PTR) meetings. Each review performs a Validation &

Verification function by including members of the technical community in the review and verification of test results. The purpose of the review is to ensure that the requirements contained in the Change Request/Change Requests approved by the Shuttle Avionics Software Control Board for implementation in an Operational Increment have been implemented correctly and verified according to approved SSP standards for Flight Software development.

**Independent Validation & Verification activity:** Any potential outstanding issues and/or concerns would be conveyed at the Configuration Inspection.

#### Mission Preparation Phase

This phase is comprised of the following steps:

##### 1. Reconfiguration Data

The Shuttle Flight Operations Contract supports NASA MOD Reconfiguration Management Division (RMD) who define the requirements and vehicle-specific data (I-loads), used to reconfigure the PASS and Backup Flight Software Operational Increment baseline loads for specific missions and vehicles.

**Validation & Verification activity:** All I-Loads are audited by I-Load owners prior to approval and after flight cycle load build for the first flight of an Operational Increment and then for those not previously audited on subsequent flights of the Operational Increment. Simulator test conditions are provided for the Shuttle Flight Operations Contract's validation (Level 8) testing. Performance tests are executed by the Shuttle Flight Operations Contract to verify the reconfigured Flight Software.

##### 2. Vehicle Cargo System (VCS) Reconfiguration Data

The Shuttle Flight Operations Contract processes data from Shuttle Transport Automated Reconfiguration (STAR) and Measurement and Stimulus (MAST) Flight Software reconfiguration tools to generate VCS software data inputs required for a mission-specific Flight Software load.

**Validation & Verification activity:** The Shuttle Flight Operations Contract verifies the data source input, checks the resulting syntax, and verifies consistency of their individual products.

##### 3. Reconfiguration Activities

The Shuttle Flight Operations Contract is responsible for developing and maintaining all software tools that can affect the reconfiguration Flight Software memory loads. At Configuration Inspection, these Flight Software build tools have completed validation and are ready for reconfiguration use.

**Validation & Verification activity:** The Shuttle Flight Operations Contract performs validation (Level 8) tests on the resulting Integrated Mass Memory Unit (IMMU).

**Independent Validation & Verification activity:** A S/W Design analysis and a Code analysis is performed utilizing the reconfiguration data prior to incorporation into the Integrated Mass Memory Unit. Any findings or recommendations are documented in a Software Independent Validation & Verification Report and are reported to the Software Readiness Review.

##### 4. Operational Validation Testing

Level 8 (Mission) testing is performed using flight equivalent interfaced with a mainframe computer containing Shuttle math models simulating the mission conditions necessary to test the Flight Software. Level 8 testing, whose requirements are controlled by the Shuttle Avionics Software Control Board in the Performance Test Plan, is conducted using the final (L-77) reconfiguration load, which contains mission-unique I-Loads. Validation testing is performed by the Shuttle Flight Operations Contract.

Operational testing is defined as the operational use of the Flight Software during mission preparation (i.e., flight and ground operations training, mission procedures development, etc.) and Shuttle Avionics Integration Laboratory (SAIL) testing. Problems found during operational testing are recorded in Change Requests, and submitted to the appropriate organization for analysis or resolution.

**Validation & Verification activity:** Crew and mission operations training in the SES and SMS exercise the man-in-the-loop Flight Software interface to validate mission capability. The Shuttle Avionics

Integration Laboratory is used to verify the integrated hardware/software interfaces as well as mission capability and the man-in-the-loop Flight Software interface testing.

**Independent Validation & Verification activity:** An analysis of the operational test planning is performed with any reported findings or recommendations going to the testing community.

#### 5. Performance Test Reviews (PTRs)

These milestones lead to the release of Flight Software for use in each Shuttle mission and are administered by distributing performance test reports to the Flight Software community for their review and concurrence.

**Validation & Verification activity:** The Flight Software community members are responsible for reviewing test result summary reports for reasonableness within their areas of accountability.

**Independent Validation & Verification activity:** An analysis of the Level 8 performance test planning is performed with any reported findings going to the testing community.

#### 6. Flight and Software Readiness Reviews

A Software Readiness Review (SRR) is conducted by NASA to allow all members of the Flight Software community to review Flight Software open issues relating to the software's ability to perform the planned mission. The results of the level 8 testing are reviewed, as well as any software issues encountered during operations. The Flight Software Readiness report is released for review to the Flight Readiness Review and any subsequent findings or recommendations not resolved at the Software Readiness Review would be reported to the Flight Readiness Review.

A Flight Readiness Review is held to resolve any remaining issues that may affect the planned mission. The Flight Readiness Review is held by the SSP to allow all the members of the STS community to review and disposition open STS hardware and software issues related to the planned mission. All aspects of flight vehicle preparation are reviewed and flight or mission-related concerns recorded and dispositioned. The Flight Software community are responsible for supporting these readiness reviews and identifying their readiness posture to support flight.

**Validation & Verification activities:** The Shuttle Flight Operations Contract and NASA Flight Software organizations having a role in preparation of Flight Software for the flight/mission are required to certify that preparations are completed and that to the best of their knowledge there are no known problems that affect the safety of the flight or completion of the STS mission.

**Independent Validation & Verification activities:** Independent Validation & Verification reports findings and makes recommendations resulting from the Mission Preparation phase to the Software Readiness Review. An Independent Validation & Verification Certificate of Flight Readiness statement is provided to the Software Readiness Review.

## Appendix 10

### Aerospace Safety Advisory Panel (ASAP) Findings: 1989 to 1998

#### Reporting and Tracking

Findings: REPORTING/TRACKING	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998
difficult to find meaningful metrics to show safety risks or unsafe conditions -- utilize procedure for finding and reporting mishaps and close calls which should produce far more significant insight into safety risks										X
principal cause of processing errors is incorrect documentation ("paper")										X
development of metrics using structured surveillance information has lagged data collection									X	
no metric for measuring impact on downsizing on safety								X		
downsizing requires NASA involvement in "out-of-family" events only-- need definition of out of family and insight into categorization by contractor							X			
improve/expand engine health monitoring					X					
SSME Health monitoring system--old technology, need to update					X					
structured surveillance, i.e., reduced reliance on inspections for quality control should be cautiously expanded (careful evaluation of structured surveillance)				X	X					
incorrectly written OMI's led to over-pressurization of a solid rocket booster hydraulic tank			X							
procedures for tracking, analyzing, and providing corrective actions are complex, lengthy, and lack overall coordination to ensure correction			X							
Shuttle Processing Data Management System (SPDMS) had not provided anticipated benefits mainly because users not involved in design process			X							
NASA does not have a system for collecting self-reports of human error that do not lead to reportable events (e.g., ASRS)			X							
mishap reporting & investigation (8621.E) should include human factors expertise and close call investigation		X								
reports indicate declining rate of incidents--concern that it may be an artifact of the reporting system		X								
cases of recurring waivers for same subsystems or component on successive flights		X								
FMEA training should be provided throughout NASA		X								
NASA's position that lack of maturity, insufficient database and lack of funds associated with quantitative risk assessment limits its usefulness	X									
Need to monitor aging and reliability of components as function of time--can't always use fleet leader stats because do not know if representative or outlier	X									
FRR, L-2, L-1 reviews should continue to be face-to-face reviews --others can be tele-, videocon	X									

**Figure 32 -- ASAP Findings: Reporting & Tracking**



**SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT**  
**FEBRUARY 9, 2000**

## Workforce

Findings: WORKFORCE	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998
potential crisis of losing core competencies to conduct spaceflight in safe and effective manner (erosion of skill/experience mix at KSC)									X	X
shortfalls in workforce training with NASA/USA can jeopardize otherwise safe operations										X
need simulation based training for launch and flight operations especially after long hiatus										X
senior managers in future will lack necessary hands-on technical knowledge and experience to provide effective insight of operations (training and experience of NASA supervisory personnel when traditional learning ladder positions are contractor)								X		X
NASA and USA making extensive use of cross training (tech&eng)-need reliable measure of readiness before performing new tasks									X	
S&MA (NASA) overseeing operations requiring SCAPE are not certified for SCAPE									X	
reduction of GMIP's lagging downsizing resulting in increased workload for NASA quality (similarly for eng and safety at KSC)									X	
cutbacks in Govt/contract personnel and resources and transition of tasks from govt to contract-new mode, should be approached cautiously and with oversight (KSC &SPC management must be vigilant in avoiding impacts on safety as a result of personnel/cost reductions)					X		X			
morale at KSC due to uncertainty of SFOC					X		X			
clear need for more operational human factors input					X					
shuttle processing problems (many) attributable to human factors					X					
NASA not utilizing resources to study safety problems relative to how human factors can improve spaceflight ground operations			X							
perception at KSC that disciplinary actions for errors are overly severe		X								

**Figure 33 -- ASAP Findings: Workforce Findings**

**SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT**  
**FEBRUARY 9, 2000**

## Operations

Findings: OPERATIONS	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998
repair turnaround times (RTAT's) are increasing--may contribute to poor reliability and mishaps (RTAT's appear to be worsening) (RTAT longer than desired due to failure analysis)		X		X	X					X
long term projections suggest increasing cannibalization rates, RTAT's and loss of repair capability (trend toward increased)						X		X	X	
although transition to SFOC satisfactory, lingering concerns include danger of not keeping safety first; tendency for success oriented environment to overlook need for open discussion; budget not allowing NASA presence on floor; need to find measure of operations and processing effectiveness									X	
return Flight Support Motor (FSM) test firings to every 12 months rather than every 18 months (reevaluate decision to have 2 years between FSM firings) (firings of FSM to check changes to RSRM being stretched out) (continue to use FSM firings for implementation of SFOC results in reduction of opportunities for NASA to maintain floor interfaces with contractor--could affect NASA assessment function)		X					X	X	X	
post flight discovery of wrench/name plate in skirt of STS-79 raises concern over QA procedures								X		
changes to processes necessary to counter obsolescence and new environmental reg's are creating problems								X		
obsolescence represents serious operation problem with potential to impact safety (obsolescence growing problem)		X					X			
SSME needs special inspection and life limits --maintain rigor even after upgrades (vigilant inspections of SSME's must be)				X		X				
TPS inspections largely quantitative and dependent on skill of need to improve effectiveness of launch processing @ KSC to reduce delays and roll backs			X							
improve coordination among task teams			X							
Pre-Challenger problems (excessive overtime, lack of clarity in work instructions, shortage of spare parts, and heavy paperwork burden) not totally eliminated	X									

**Figure 34 -- ASAP Findings: Operations Findings**

## Appendix 11

### Historical Trends

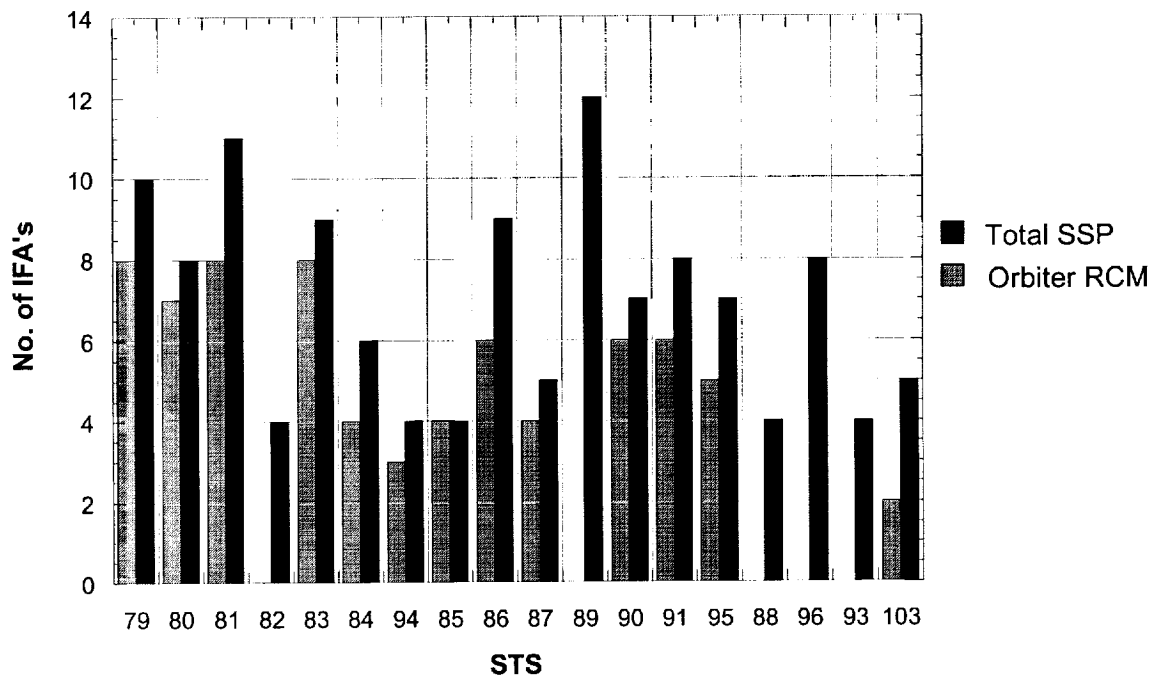


Figure 35 -- Space Shuttle In-Flight Anomalies

The SIAT did not identify a single, ideal metric in the information presented by the SSP to indicate the effects of aging and the adequacy of maintenance efforts in addressing these effects. IFA's (see *Figure 35*) were used as an indication of how many actual problems develop during flight that may affect flight safety and mission completion. The number of Problem Reports generated during Shuttle maintenance periods was also examined (see **Problem Reporting & Tracking Process**); however, PR generation is affected by a number of factors, including the number of inspectors and inspection points and the adherence to reporting procedures, that may obscure the number of actual problems. A third metric, the history of open Corrective Action Reports (CAR's) was studied as well (see *Figure 36*). The number of open CAR's is indicative of both the number of problems and the effectiveness of the resolution process. Missing from all three indicators is explicit information concerning the severity of the problems. As a consequence, some combination of these metrics (and others) should be examined, with the appropriate analyses to identify the true trends and their root causes.

SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT  
FEBRUARY 9, 2000

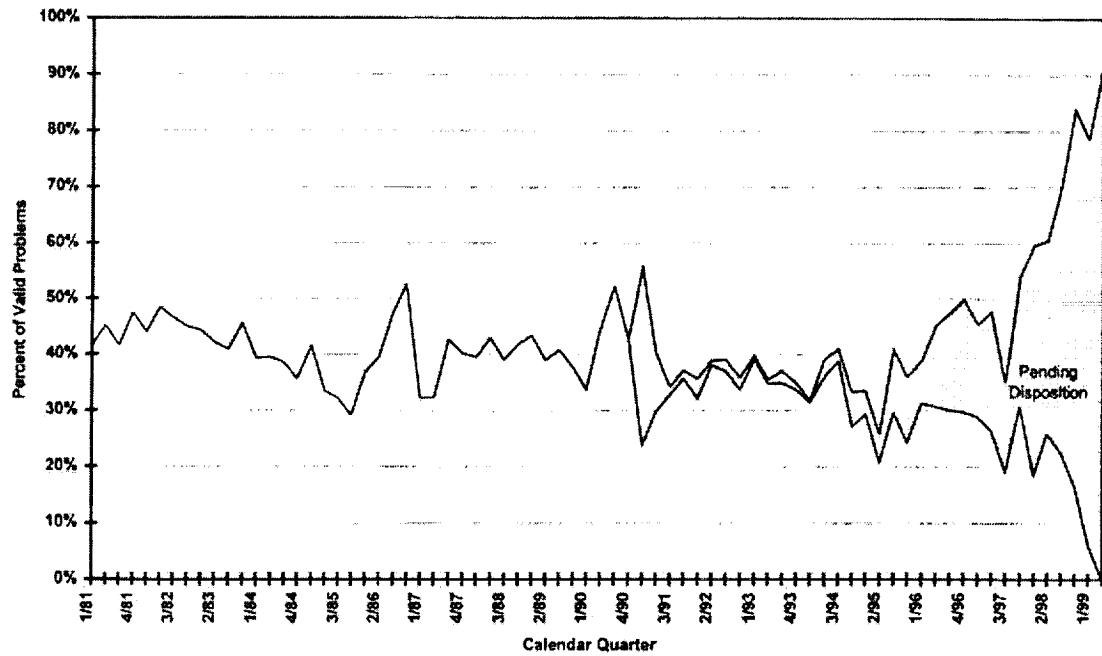


Figure 36 -- Corrective Action Report History

## Appendix 12

### SIAT Members: Backgrounds

#### **Henry McDonald**

Director, NASA Ames Research Center  
Independent Assessment Team Chairman

Dr. Henry McDonald became Director of the Ames Research Center, Mountain View, CA, on March 4, 1996. McDonald, formerly the Assistant Director of Computational Sciences and Professor of Mechanical Engineering at the Applied Research Laboratory, Pennsylvania State University, earned his bachelor's degree in aeronautical engineering and doctorate in engineering from the University of Glasgow, Scotland. McDonald has authored and reviewed many papers on aeronautical research and development. He is a Fellow of the American Institute for Aeronautics and Astronautics, a Fellow of the American Society of Mechanical Engineers, and a Fellow of the Royal Aeronautics Society of the United Kingdom. In 1997, Dr. McDonald was awarded the NASA Medal for Outstanding Leadership.

#### **Michael T. Conahan**

Technical Consultant

Mr. Conahan recently retired after many years in heritage Douglas Service Engineering (Customer Support). He currently works with Service Engineering on a technical consultant basis. He also continues to act as the heritage Douglas focal on the aging systems working group that reports to the Aging Systems Advisory Committee for Boeing Commercial Aircraft. This working group is responsible for the non-intrusive wiring survey of airplanes that are 20 years old. Mr. Conahan has years of detailed experience inspecting wiring in airplanes.

#### **Donald Eaton, RADM, USN (Ret.)**

Logistics Chair, Systems Management Department, Naval Postgraduate School

Admiral Donald R. Eaton is the Logistics Chair in the Systems Management Department of the Naval Postgraduate School. He is a Senior Lecturer for Logistics and related fields. He retired from the Navy as a Rear Admiral on 1 January 1994 after serving for more than 36 years. He has more than 2500 hours of operational experience in A-3 and A-6 naval attack aircraft as a Bombardier/Navigator and flew combat in Vietnam. During his combat tour he flew 66 combat missions and on 14 July 1965, he and his pilot, Admiral Donald V. Boecker, were shot down near Sam Neua, Laos. After successfully evading enemy troops for a night and a day, they were rescued by an Air America H-34 helicopter.

Admiral Eaton has extensive experience in Naval Aircraft Maintenance and Logistics assignments and has served as a Squadron maintenance officer and Director of Intermediate Maintenance Activities. He also was the Director of Naval Aviation Depot Maintenance activities and was the Director of Logistics and Fleet Support for Naval and Marine Corps aviation. He has also served as the Director of Space and Sensor Systems and Executive Assistant and Naval Aide to the Assistant Secretary of the Navy for Research and Development.

He has a Bachelor of Science in Engineering Science from the Naval Postgraduate School and a Master of Science from George Washington University. He is also a graduate of the Industrial College of the Armed Forces and The Naval Aviation Safety Officer's School.

His decorations include the Distinguished Service Medal, four Legions of Merit, the Purple Heart, five Air Medals, four Navy Commendation Medals (three with Combat V) and the Combat Action Ribbon.

### **Robert Ernst**

Deputy for Research & Development Ownership Cost Reduction Efforts, Naval Air Systems Command, Patuxent River, MD

Mr. Ernst earned his bachelor's degree in Aerospace Engineering from the University of Maryland, and began his professional career in the Aerodynamics and Flight Controls Branch, where he was responsible for developing computer based analysis of aircraft performance and air combat maneuvering. Following involvement in the F-14D engine selection and Adversary Aircraft Programs, Mr. Ernst joined the Systems Engineering Division as F-14 Project Engineer where he was responsible for a series of avionics upgrades and structural modifications.

In 1986, Mr. Ernst was selected as the Sr. Project Engineer for the S-3 and ES-3 Programs, responsible for design, development, test and evaluation of the ES-3 Modification Program. He directed a series of operational and service life improvements for both weapon systems including the creation of a Service Life Assessment Program and a series of critical avionics upgrades to counter the effects of increasing avionics obsolescence and poor reliability. In addition, he was designated Deputy Program Manager for S-3 avionics in 1998.

In March of 1999, Mr. Ernst was selected to head the newly established Aging Aircraft Program and currently serves as the Deputy for Research and Development Ownership Cost Reduction Efforts. He coordinates all R&D funding directed to countering the effects of aging aircraft, and coordinating age studies and investigations with the Federal Aviation Administration, Air Force and NASA.

Mr. Ernst is a 1996 graduate of the Defense Systems Management College, Advanced Program Manager's Course. His awards include runner up for the Navy Streamlining Award in 1989 and Competition in Contracting award in 1994. In 1996 he was awarded the Meritorious Service Medal.

### **George Hopson**

Project Manager, Space Shuttle Main Engine (SSME), NASA Marshall Space Flight Center

Mr. Hopson holds Bachelor and Master of Science degrees in mechanical engineering from the University of Alabama. Mr. Hopson began his engineering career in 1954 and was a senior propulsion engineer for General Dynamics Corporation before joining the Marshall Space Flight Center in 1962.

He was Chief of the Fluid and Thermal Systems Branch in the Propulsion Division of the Center's former Astronautics Laboratory and became Chief of the Engineering Analysis Division of the Structures and Propulsion Laboratory. From 1979-1981 he served as Director, Systems Dynamics Laboratory. He was selected as Director of the Systems Analysis and Integration Laboratory in 1981, serving in this position for seven years. He was appointed as Associate Director for Space Transportation Systems. In January 1989, he assumed the position of Manager of the Space Station Projects Office at Marshall. He served in this position for five years before becoming Deputy Director for Space Systems in the Science and Engineering Directorate at Marshall. In this position, he supervised the Chief Engineering Offices with regard to both manned and unmanned space systems before receiving the current assignment in 1997.

## **Barbara Kanki**

Crew Factors Team Leader, NASA Ames Research Center

Dr. Kanki, (PhD in Behavioral Sciences from the University of Chicago) joined the Human Factors Division at NASA Ames Research Center 14 years ago as a principal investigator of crew factors in aviation and space systems. Her initial work focused on aircrew communication and coordination in support of Crew Resource Management training. This work expanded to other parts of the aviation system including air traffic management (e.g., pilot-controller communication) and aircraft maintenance (e.g., Maintenance Resource Management). Currently Dr. Kanki is the technical manager of the Maintenance Human Factors element of the NASA Aviation Safety Program and coordinates this program of research with government and industry partners, including the Federal Aviation Administration, the Air Transport Association, airlines, manufacturers, unions and international counterparts. In this capacity, she has encouraged the technology transfer of maintenance human factors in aviation to ground operations in space systems, namely payload, launch and Shuttle processing. Other current projects include crew research sponsored by the Federal Aviation Administration Air Carrier Training Program, NASA's Terminal Area Productivity Program, and NASA's Human Reliability Program. She has conducted human factors and communication analyses for NTSB investigations (Pegasus incident report 1993 and USAir 427 accident report 1999), and has a longstanding consultative role to the nuclear power industry.

## **John Lahoff, Lt.Col., USAF**

Program Director, Space Safety, Directorate of Nuclear Surety, Weapons, & Space Safety, HQ Air Force Safety Center, Kirtland AFB

Lt. Col. Lahoff attended the United States Air Force Academy (USAFA) and graduated in May 1980 with a Bachelor of Science Degree in Aviation Science.

He entered Minuteman Missile Operations entered the missile operations career field and served in various Missile Combat Crew Commander positions until May 1985. While there, he earned a Master of Science Degree in Safety from Central Missouri State University in 1983 and completed Squadron Officer School in residence in 1985 before heading to the Air Force Institute of Technology (AFIT) in 1985.

At the Graduate Logistics Management program at Wright Patterson AFB, OH, Lt. Col. Lahoff earned a Masters of Science Degree. Later he assumed duties as the OIC, Missile Electrical Branch, Maintenance Supervisor in at a Missile Maintenance Squadron and Chief, Training Control Division. Following this assignment at Grand Forks AFB, he moved to Headquarters Air Combat Command at Langley AFB, VA and was assigned to the Civil Engineering Directorate's Technical Support Office, Missile Engineering Division.

He assumed his current position in August 1998. Lt. Col. Lahoff's military decorations include the Air Force Meritorious Service Medal (two oak leaf clusters) and the Air Force Commendation Medal (two oak leaf clusters).

## **John McKeown**

Deputy for Systems Engineering, Naval Air Systems Command, Patuxent River, MD

Mr. McKeown earned his bachelor's degree from Pennsylvania State University and holds graduate degrees from the University of Northern Colorado and the John F. Kennedy School at Harvard University. Mr. McKeown began his professional career at Sikorsky Aircraft, and then entered government service at the Naval Weapons Laboratory as supervisor, Aircraft Systems Section. His responsibilities included weapon systems integration, airborne fire control, and systems software evaluation. Starting in 1975 he managed modernization and development programs at the Naval Air Systems Command, and later assumed the position of Head, Flight Controls Branch and was responsible for flight control engineering research and development.

Now, Mr. McKeown oversees the conversion of mission needs into technical requirements for the Navy through an integrated, balanced engineering effort which meets cost, schedule and performance objectives across the entire aircraft life cycle.

Mr. McKeown served on the Congressional Aeronautics Advisory Committee and is a member of the American Helicopter Society in which he served on its Handling Qualities Committee and Technical Council. He is an active participant in the National Rotorcraft Technology Center and a Board Member of the Rotorcraft Industry Technology Association, and is a private pilot.

### **James C. Newman, Jr.**

Senior Scientist, Mechanics and Durability Branch, NASA Langley Research Center

Dr. Newman received his bachelor's in Civil Engineering in 1964 from the University of Mississippi and his master's and PhD in Engineering Mechanics in 1969 and 1974, respectively, from the Virginia Polytechnic Institute and State University.

In 1964, he began his career at the NASA Langley Research Center in the area of fatigue and fracture of metallic materials. He is a member and past officer in the American Society for Testing and Materials (ASTM) Committee E-08 on Fatigue and Fracture. He has been the chairman or co-chairman of 9 national or international symposia on fatigue and fracture; and has edited or co-edited 9 books (ASTM Special Technical Publications). He has over 120 publications in journals and NASA reports. From 1980 to 1993, he worked on several teams to investigate problems in the Space Shuttle Transportation System (Thermal Protection System, Solid Rocket Motor, and the External Tank). During the 1990's, he was the technical manager of the fatigue and fracture research in the NASA Airframe Structural Integrity Program. He has received numerous awards and medals from NASA and ASTM.

Currently, Dr. Newman is conducting research on experimental and computational aspects of crack behavior to develop material databases, models and theories for fatigue life, durability and damage tolerance analyses of aging commercial aircraft and future high-speed civil transport structures.

### **Robert Sackheim**

Assistant Director for Space Propulsion Systems, NASA Marshall Space Flight Center

Mr. Sackheim oversees all advanced space propulsion activities at Marshall Space Flight Center. In his new role, Sackheim provides technical expertise to all activities focused on the exploration of space — including new and innovative propulsion system development at Marshall. Mr. Sackheim holds a master's degree in chemical engineering from Columbia University in New York, and has completed all doctoral coursework in chemical engineering at the University of California in Los Angeles.

He served as manager of the Propulsion Systems Center in the Space and Technology Division of TRW Corp. where he was responsible for design, development and testing of new propulsion, combustion and fluid system products and materials technology.

He joined TRW in 1964 as project manager for the Mariner Mars Propulsion Sub-system and achieved special recognition in 1983 when he led the propulsion team responsible for enabling the rescue of NASA's Tracking and Data Relay Satellite, following a malfunction of the Inertial Upper Stage injection vehicle. In 1986, Mr. Sackheim became project manager of the Orbital Maneuvering Vehicle Propulsion Modules Project, where he was responsible for design, testing, flight performance and operations planning. He has authored more than 100 technical papers and holds seven patents in spacecraft control and propulsion systems technology. His awards and honors include the James C. Wyld Award for Outstanding Technical Contributions to the Field of Rocket Propulsion, as well as three NASA Group Achievement Awards. In 1997, he was elected to the International Academy of Astronautics, and continues to serve on two National Research Council committees on Space Science and Technology.



## **George Slenski**

Team Leader, Electronic Materials Evaluation Group, Air Force Research Laboratory, Wright-Patterson AFB

Mr. Slenski is the Lead engineer in electronic materials evaluation group responsible for planning, organizing, and conducting electronic failure analysis on fielded and new systems. Responsibilities also include using failure analysis insight to develop and manage programs that improve and enhance aerospace systems. He is the Program Manager for developing a new aerospace wire insulation, development of a handbook for conducting electrically related mishap investigations, and for developing a life prediction system for aging wiring systems.

His specific expertise includes microelectronics failure analysis techniques, mishap investigation techniques related to electronics, wire insulation, and electromechanical devices. Some of his recent activities include testifying as a wiring expert on the TWA 800 aircraft accident and participating in the Federal Aviation Administration aging aircraft sub-committee on wiring inspection. Current emphasis area is on characterizing and assessing aging electronic systems, specifically dealing with wiring and connectors.

Mr. Slenski holds a Master of Science in Materials Engineering from the University of Dayton, and a Bachelor of Science in Electrical Engineering from the University of Florida.

## **Randall Strauss, Col., USAF**

Chief, Weapons, Space & Nuclear Safety Division, HQ Air Force Safety Center, Kirtland AFB

Colonel Strauss holds a Master of Arts degree in Government from Georgetown University and is a graduate of the USAF Air War College, class of 1994. He is experienced in aging aircraft sustaining activities and organizational outsourcing and privatization. Prior to his current assignment, he was Commander, 325th Logistics Group, 325th Fighter Wing, the USAF's F-15 training unit. In 1997-99 he converted the logistics group from a five squadron structure of 1,200 military and civil service personnel to one composed of two major contractors and a substantially reduced number of Air Force personnel.

He is a career logistics officer, wearing master aircraft and munitions maintenance, senior missile maintenance, and senior explosive ordnance disposal officer badges. His military decorations include the Legion of Merit.

## **John Young**

Associate Director (Technical)

Mr. Young received a Bachelor degree in Aeronautical Engineering with highest honors from the Georgia Institute of Technology in 1952. Upon graduation he entered the United States Navy and after test pilot training he was assigned to the Naval Air Test Center for 3 years. Prior to reporting to NASA, he was a maintenance officer. He retired from the Navy as a Captain in September 1976, after completing 25 years of active military service.

Mr. Young served as Chief of the Astronaut Office until May 1987, and later as Special Assistant to the Director of Johnson Space Center for Engineering, Operations, and Safety. In his current role, he is responsible for technical, operational and safety oversight of all Agency Programs and activities assigned to the Johnson Space Center. As an active astronaut, Young remains eligible to command future Shuttle astronaut crews.

He has received multiple honors and awards, including the Congressional Space Medal of Honor, NASA Distinguished Service Medal, NASA Outstanding Leadership Medal, NASA Exceptional Engineering Achievement Medal, NASA Outstanding Achievement Medal, Navy Astronaut Wings, Navy Distinguished Service Medal, Navy Distinguished Flying Cross, Georgia Tech Distinguished Service Alumni Award, Exceptional Engineering Achievement Award, Academy of Distinguished Engineering Alumni, and the American Astronautical Society Space Flight Award.

## Appendix 13

### Historical Shuttle Flight Manifest

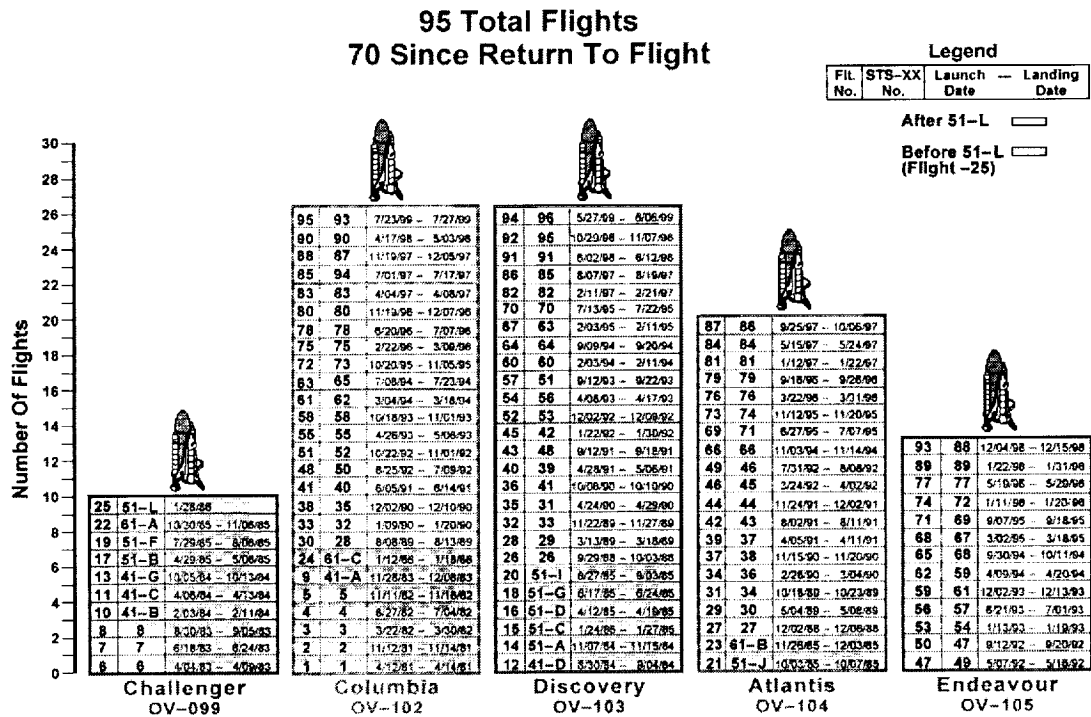


Figure 37 -- Shuttle Flights Through 7/99

## Appendix 14

### Orbiter Zones

Major zone numbering designations for the Orbiter vehicle are as follows:

- 100 - Forward Fuselage
- 200 - Mid-fuselage
- 300 - Aft Fuselage and Body Flap
- 400 - Vertical Stabilizer
- 500 - Propulsion and Reaction Control System
- 600 - Right Wing
- 700 - Left Wing
- 800 - Nose Cap, Hatches, and Doors
- 900 - Landing Gear and Landing Gear Doors

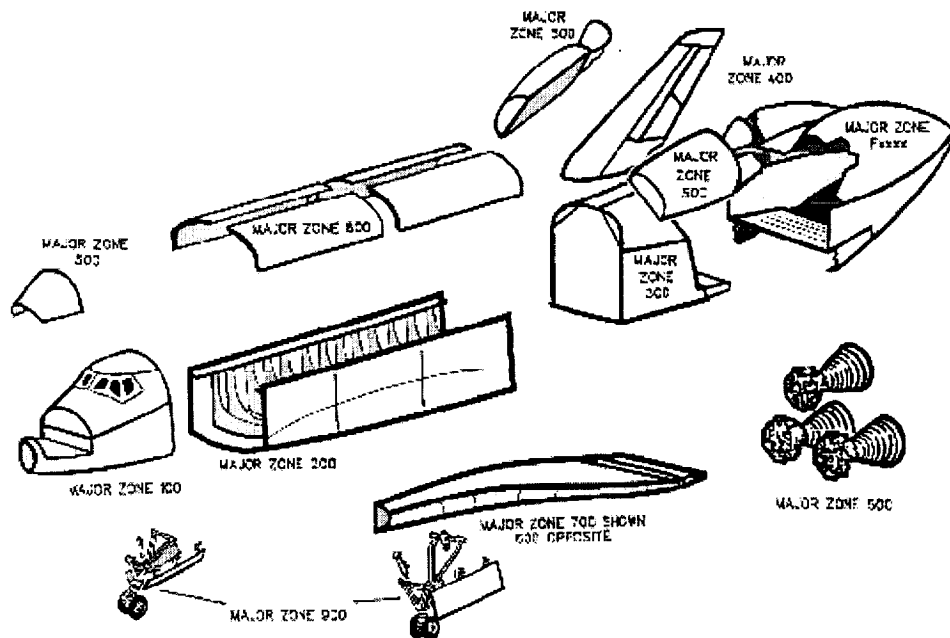
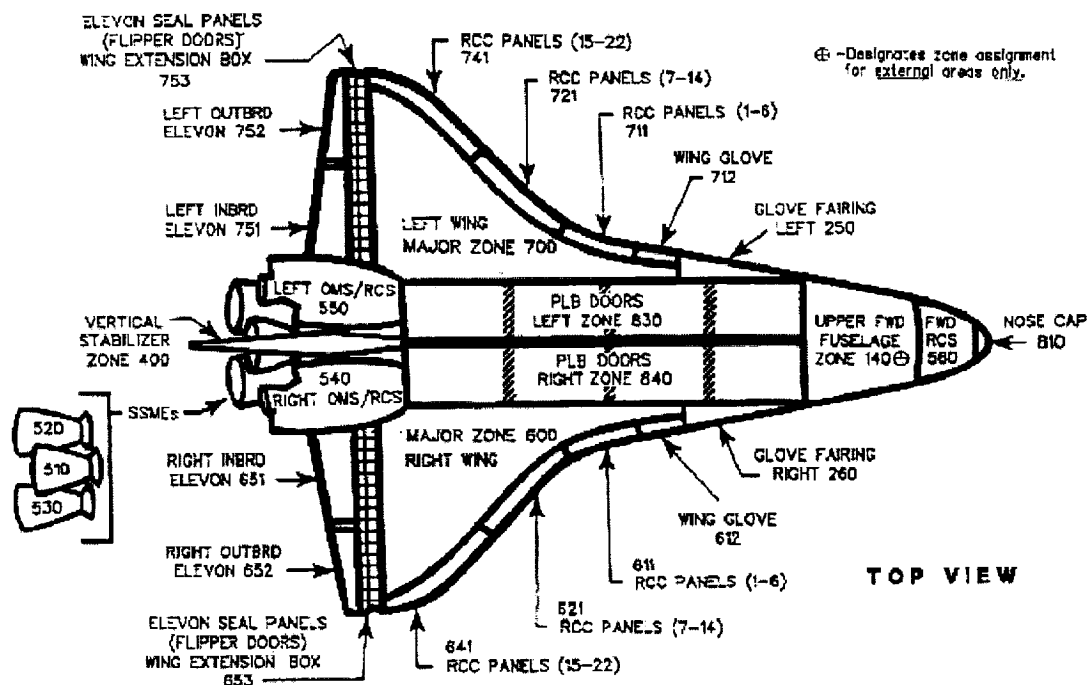
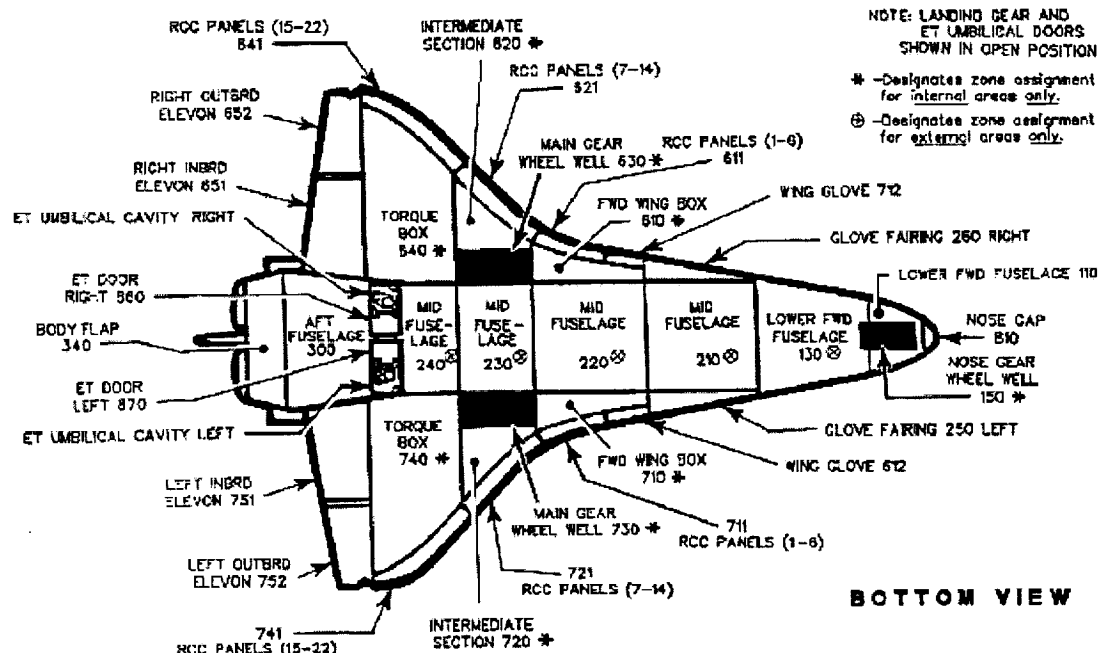


Figure 38 -- Orbiter Zones Exploded View

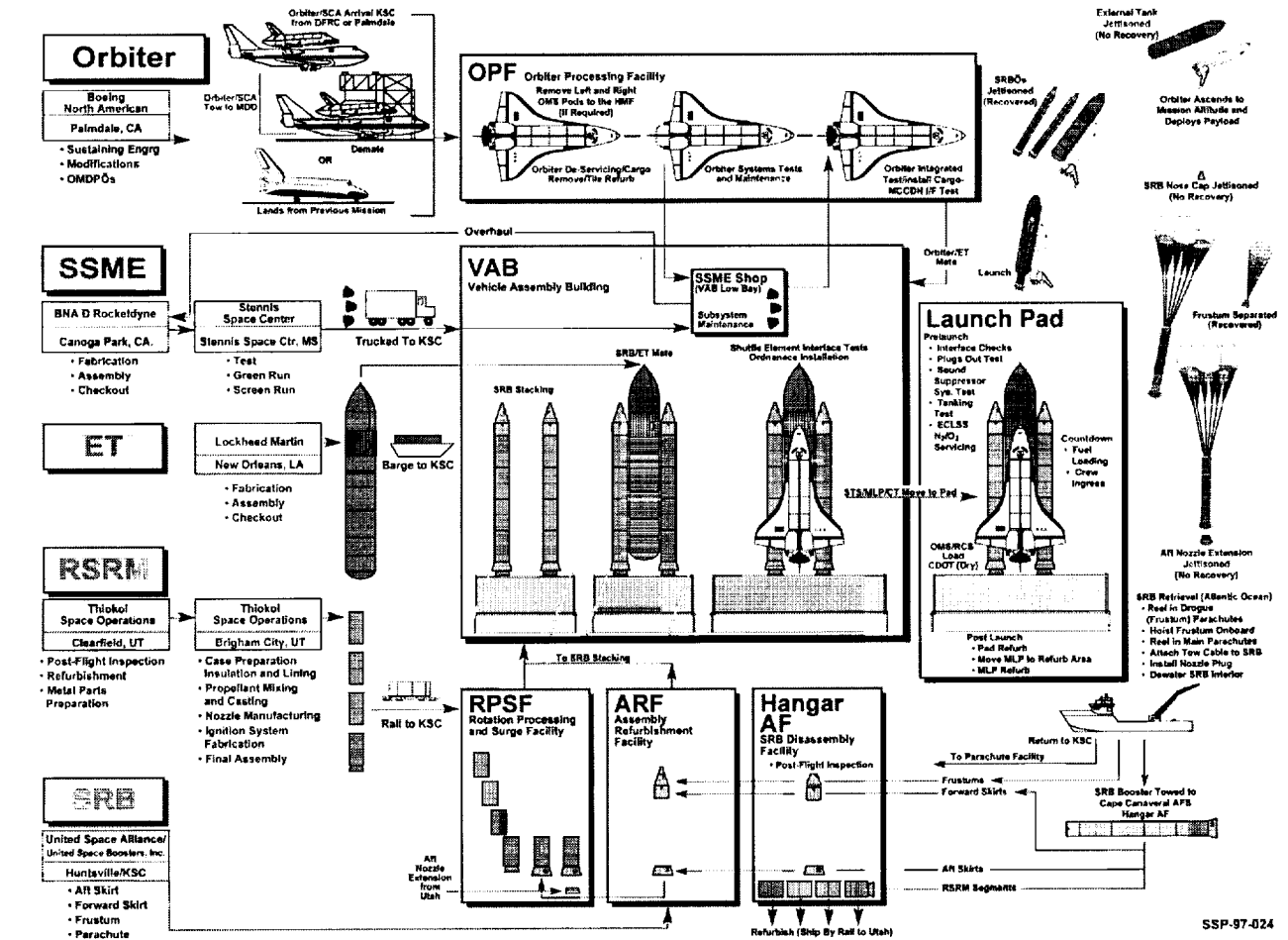
**SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT**  
**FEBRUARY 9, 2000**



**Figure 39 -- Orbiter Zones: Top View**



## Appendix 15



060999\_03flow

## Space Shuttle Hardware Flow

## Appendix 16

### Acronyms & Glossary

ASAP	Aerospace Safety Advisory Panel
APU	Auxiliary Power Unit
CAR	Corrective Action Record
CB	Circuit Breaker
CCB	Configuration Control Board
CCRB	Corrosion Control Review Board
CIL	Critical Items List
CLCS	Checkout & Launch Control System
CoFR	Certificate of Flight Readiness
CPCP	Corrosion Prevention and Control Plan
CR	Change Request
CRIT	Criticality
Diving Catches	Problem caught before launch but process did not catch it -- an individual performed a "heroic effort".
DR	Discrepancy Report
EPU	Emergency Power Unit
Escape	Something that flew that could have caused a failure; luck or providence prevented it.
ET	External Tank
FAA	Federal Aviation Administration
FARS	Federal Aviation Regulations
FCP	Flight (Software) Change Proposal
FDF	Flight Data File
FMEA	Failure Modes and Effects Analysis
FOD	Foreign Object Debris
FPP	Flight Preparation Process
FRCS	Forward Reaction Control System (RCS)
FRR	Flight Readiness Review
FSW	Flight Software
FTA	Fault-Tree Analysis
FTR	Fracture-Toughness Ratio
GIDEP	Government Industry Data Exchange Program
GMIP	Government Mandatory Inspection Point
GNC	Guidance, Navigation and Control
GSE	Ground Support Equipment
HA	Hazards Analysis
HEDS	Human Exploration & Development of Space
HMF	Hypergol Maintenance Facility
HPFTP/AT	Alternate High-Pressure Fuel Turbopump
HPOTP/AT	Alternate High-Pressure Oxidizer Turbopump
IFA	In-Flight Anomaly

**SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT**  
**FEBRUARY 9, 2000**

---

IFOD	Internal Foreign Object Debris
IV&V	Independent Validation & Verification
JSC	Johnson Space Center
KSC	Kennedy Space Center
LRU	Line Replaceable Unit
MCC	Main Combustion Chamber
MECO	Main Engine Cut-Off
MRB	Material Review Board
MSFC	Marshall Space Flight Center
MTBF	Mean Time Between Failures
MVP	Master Verification Plan
NDE	Non-Destructive Evaluation
NSLD	NASA Shuttle Logistics Depot
NSTS	National Space Transportation System
OBITS	Onboard Integrated Testing System
OI	Operational Increments
OME	Orbital Maneuvering Engine
OMI	Operations and Maintenance Instruction
OMRSD	Operational Maintenance Requirements and Specifications Document
OMS	Orbiter Maneuvering System
OPF	Orbiter Processing Facility
OSF	Office of Space Flight
PCASS	Program Compliance Assurance and System Status
PMRB	Primary Material Review Board
PR	Problem Report
PRA	Probabilistic Risk Assessment
PRACA	Problem Resolution and Corrective Action
PRCB	Program Requirements Control Board
PRT	Prevention/Resolution Team
PTR	Performance Test Review
QRAS	Quantitative Risk Assessment System
RCN	Requirements Change Notice
RCS	Reaction Control System
RMP	Risk Management Plan
RSI	Reusable Surface Insulation
RSRM	Reusable Solid Rocket Motor
S&MA	Safety & Mission Assurance
SAIL	Shuttle Avionics Integration Laboratory
SCAPE	Self-Contained Atmospheric Protective Ensemble
SFOC	Shuttle Flight Operations Contract
SFR	Single Flight Reliability
SIAT	Space Shuttle Independent Assessment Team
SIR	Software Independent Validation & Verification Report
SLWT	Super Light-Weight Tank
SPC	Statistical Process Control
SPR	Suspect Problem Report
SRB	Solid Rocket Booster
SRR	Software Readiness Review
SRU	Shop Replaceable Unit
SSME	Space Shuttle Main Engine

**SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT**  
**FEBRUARY 9, 2000**

---

SSP	Space Shuttle Program
SSR	System Safety Review
STAR	Shuttle Transport Automated Reconfiguration
STE	Special Test Equipment
TCT	Test Coordination Team
TPS	Thermal Protection System
TT&E	Test, Teardown and Evaluation
TVC	Thrust Vector Control
USA	United Space Alliance
V&V	Validation & Verification
VTP	Verification Test Procedures



## Section 7 - References

---

- <sup>1</sup> Haimes, Yacob Y., Risk Modeling, Assessment, and Management, p. 20, 1998.
- <sup>2</sup> Presentation to Code M: KSC Workforce Issues, October 29, 1999.
- <sup>3</sup> Air Transport Association (ATA) Specification 113, Chapter 3
- <sup>4</sup> Lockheed-Martin, Titan IV Investigation, 1999.
- <sup>5</sup> EWR 127-1, Eastern and Western Range Safety Requirements
- <sup>6</sup> Pate-Cornell, M. E., Organizational Aspects of Engineering Systems Safety: The Case of Off-Shore Platforms, Science Vol. 250, pp. 210-217, 1990.
- <sup>7</sup> Haimes, Yacob Y., Risk Modeling, Assessment, and Management, p. 21, 1998
- <sup>8</sup> Boeing, Procedures for Orbiter Problem Reporting and Corrective Action (PRACA), October, 1997.
- <sup>9</sup> Johnson Space Center Safety Reliability and Quality Assurance, Orbiter CFE Problem Trend Analysis Report, September 15, 1999.
- <sup>10</sup> Space Flight Operations Contract (SFOC), NAS9-20000, Attachment J-1-A-6: Statement of Work (SOW), Section 1.1.1.4, Risk Management.
- <sup>11</sup> Space Flight Operations Contract (SFOC), NAS9-20000, Data Requirement Description (DRD) 1.1.1.4-a, Space Shuttle Program risk Management Plan.
- <sup>12</sup> Space Flight Operations Contract (SFOC), NAS9-20000, Data Requirement Description (DRD) 1.1.1.4-b, "Risk Assessment.
- <sup>13</sup> Space Shuttle Program Risk Management Plan, SFOC-PG9604, April 1, 1997.
- <sup>14</sup> United Space Alliance, Independent Review of Orbiter, Sub-systems, & Maintenance Processes, December, 1999.
- <sup>15</sup> Report to the President by the Presidential Commission on the Space Shuttle Challenger Accident, June 1986.
- <sup>16</sup> Space Division, Rockwell International, Contract NAS9-14000, Space Shuttle Orbiter Fracture Control Plan, SD73-SH-0082A, September 1974.
- <sup>17</sup> Boeing – Palmdale and United Space Alliance (USA), OV104 V30/V31 Inspection Report, An Assessment of the Structural Inspection Findings Conducted during the J2 Modification of Atlantis, November 1997 – September 1998, 1998.
- <sup>18</sup> Orbiter Corrosion Control Review Board, Space Shuttle Orbiter Corrosion, 1981-1993, A Review and Analysis of Issues Involving Structures and Sub-systems, NASA TM 104810, June 1995.
- <sup>19</sup> NASA, KSC-MSL-0729-1999
- <sup>20</sup> <http://www.sae.org/technicalcommittees/ae8taq.htm>
- <sup>21</sup> Paulos, T. and Apostolakis, G., A Methodology to Select a Wire Insulation for Use in Habitable Spacecraft, *Risk Analysis*, Vol. 18, No. 4, 1998.
- <sup>22</sup> Friedman, R., Fire Safety Practices and Needs in Human-Crew Spacecraft, *Journal Applied Fire Safety*, Vol. 2, 1992/3, pp. 243-359.
- <sup>23</sup> Friedman, R., Risks and Issues in Fire Safety on the Space Station, NASA TM-1064033, March 1994.
- <sup>24</sup> 1<sup>st</sup>. NASA Workshop on Wiring for Space Applications, NASA Conference Publication 10145, p. 13, July, 1991.
- <sup>25</sup> 3<sup>rd</sup>. NASA Workshop on Wiring for Space Applications, NASA Conference Publication 10177, p. 10, July, 1995
- <sup>26</sup> Noer, D., Healing the Wounds: Overcoming the Trauma of Layoffs and Revitalizing Downsized Organizations, 1993
- <sup>27</sup> NASA Aviation Safety Program, L3 Plan 2.2.2 Maintenance Human Factors, 1999.
- <sup>28</sup> Air Transport Association (ATA) Specification 113, Chapter 6.
- <sup>29</sup> Air Transport Association (ATA) Specification 113, Chapter 4.

**SHUTTLE INDEPENDENT ASSESSMENT TEAM REPORT**  
**FEBRUARY 9, 2000**

---

<sup>30</sup> Independent Assessment of Shuttle Processing Directorate: Engineering and Management Processes, Final Report, November 4, 1999.

<sup>31</sup> Air Transport Association (ATA) Specification 113

<sup>32</sup> NSTS 07700, Space Shuttle Flight and Ground System Specification, Vol. X, para. 3.2.10

<sup>33</sup> NSTS 07700, Space Shuttle Flight and Ground System Specification, Vol. X, para. 3.2.10

<sup>34</sup> NSTS 08117, Requirements and Procedures for Certification of Flight Readiness.

<sup>35</sup> NSTS 08171, Operations and Maintenance Requirements and Specifications.

<sup>36</sup> NSTS 5300.4 (1D-2) Safety, Reliability, Maintainability, and Quality Assurance Provisions for the SSP.

<sup>37</sup> Space Shuttle Flight And Ground Software Verification And Validation Requirements, NSTS 08271, Revision A, January 20, 1994.

This page intentionally left blank